

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 7月11日
Date of Application:

出願番号 特願2003-195626
Application Number:

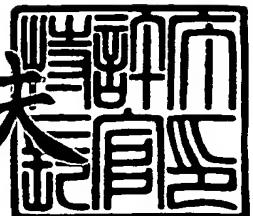
[ST. 10/C] : [JP2003-195626]

出願人 株式会社リコー
Applicant(s):

2003年12月5日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願
【整理番号】 0300734
【提出日】 平成15年 7月11日
【あて先】 特許庁長官 太田 信一郎 殿
【国際特許分類】 G06F 12/00
【発明の名称】 プログラム改ざん検証方法、カプセル化文書構造、記憶媒体、カプセル化文書作成装置、改ざん検証装置、カプセル化文書作成処理プログラム、これを記憶する記憶媒体、起動プログラム及びこれを記憶する記憶媒体
【請求項の数】 32
【発明者】
【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内
【氏名】 長谷川 雄史
【発明者】
【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内
【氏名】 鈴木 明
【発明者】
【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内
【氏名】 小出 雅巳
【特許出願人】
【識別番号】 000006747
【氏名又は名称】 株式会社リコー
【代表者】 桜井 正光
【代理人】
【識別番号】 100101177
【弁理士】
【氏名又は名称】 柏木 慎史
【電話番号】 03(5333)4133

【選任した代理人】

【識別番号】 100102130

【弁理士】

【氏名又は名称】 小山 尚人

【電話番号】 03(5333)4133

【選任した代理人】

【識別番号】 100072110

【弁理士】

【氏名又は名称】 柏木 明

【電話番号】 03(5333)4133

【手数料の表示】

【予納台帳番号】 063027

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9808802

【包括委任状番号】 0004335

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 プログラム改ざん検証方法、カプセル化文書構造、記憶媒体、カプセル化文書作成装置、改ざん検証装置、カプセル化文書作成処理プログラム、これを記憶する記憶媒体、起動プログラム及びこれを記憶する記憶媒体

【特許請求の範囲】

【請求項 1】 文書上での表現実体となる文書情報ファイルと、当該文書情報ファイルを表現実体化させる動作プログラムファイルとが少なくともカプセル化されているカプセル化文書ファイルにおける前記動作プログラムファイルの改ざん検証処理を情報処理部により実行するプログラム改ざん検証方法であって、

前記文書情報ファイルの表現実体化に際して前記カプセル化文書ファイル内の前記動作プログラムファイルの特徴量を算出するステップと、

予め保持しておいた前記動作プログラムファイルの暗号化特徴量を復号化するステップと、

復号化した前記動作プログラムファイルの特徴量と算出された前記動作プログラムファイルの特徴量とを比較するステップと、

特徴量が一致しない場合に、前記動作プログラムファイルによる前記文書情報ファイルの表現実体化を制限するステップと、

を具備するプログラム改ざん検証方法。

【請求項 2】 文書上での表現実体となる文書情報ファイルと、当該文書情報ファイルを表現実体化させる動作プログラムファイルの保存位置を示す位置情報とが少なくともカプセル化されているカプセル化文書ファイルにおける前記動作プログラムファイルの改ざん検証処理を情報処理部により実行するプログラム改ざん検証方法であって、

前記文書情報ファイルの表現実体化に際して前記カプセル化文書ファイル内に保持された位置情報に存在する前記動作プログラムファイルの特徴量を算出するステップと、

予め保持しておいた前記動作プログラムファイルの暗号化特徴量を復号化するステップと、

復号化した前記動作プログラムファイルの特徴量と算出された前記動作プログ

ラムファイルの特微量とを比較するステップと、
特微量が一致しない場合に、前記動作プログラムファイルによる前記文書情報
ファイルの表現実体化を制限するステップと、
を具備するプログラム改ざん検証方法。

【請求項3】 各種ファイルで構成されるファイル群と、
このファイル群を構成する所定のファイルに関する暗号化された特微量を保持
する特微量保持ファイルと、
をカプセル化手段によってカプセル化したカプセル化文書構造。

【請求項4】 文書上での表現実体となるコンテンツ情報である文書情報フ
ァイルと、
この文書情報ファイルを表現実体化させる動作プログラムである動作プログラ
ムファイルと、
この動作プログラムファイルに関する暗号化された特微量を保持する特微量保
持ファイルと、
をカプセル化手段によってカプセル化したカプセル化文書構造。

【請求項5】 文書上での表現実体となるコンテンツ情報である文書情報フ
ァイルと、
この文書情報ファイルを表現実体化させる動作プログラムである動作プログラ
ムファイルの保存位置を示す位置情報と、
前記動作プログラムファイルに関する暗号化された特微量を保持する特微量保
持ファイルと、
をカプセル化手段によってカプセル化したカプセル化文書構造。

【請求項6】 文書上での表現実体となるコンテンツ情報である文書情報フ
ァイルと、
この文書情報ファイルを表現実体化させる動作プログラムであり、特微量が外
部に保持されている動作プログラムファイルと、
をカプセル化手段によってカプセル化したカプセル化文書構造。

【請求項7】 文書上での表現実体となるコンテンツ情報である文書情報フ
ァイルと、

この文書情報ファイルを表現実体化させる動作プログラムであり、特微量が外部に保持されている動作プログラムファイルの保存位置を示す位置情報と、をカプセル化手段によってカプセル化したカプセル化文書構造。

【請求項8】 前記特微量保持ファイルには、前記文書情報ファイルに関する暗号化された特微量も保持されている、
請求項3ないし5の何れか一記載のカプセル化文書構造。

【請求項9】 前記特微量保持ファイルには、前記動作プログラムファイルに関する暗号化された特微量に対応付けられて前記暗号化された特微量を復号化する復号化鍵情報が保持されている、
請求項3ないし5の何れか一記載のカプセル化文書構造。

【請求項10】 前記特微量保持ファイルには、前記動作プログラムファイルに関する暗号化された特微量に対応付けられて前記暗号化された特微量を復号化する復号化鍵情報の保存位置を示す位置情報が保持されている、
請求項3ないし5の何れか一記載のカプセル化文書構造。

【請求項11】 各動作プログラムファイル毎に異なる前記復号化鍵情報が対応付けられている、
請求項9または10記載のカプセル化文書構造。

【請求項12】 前記動作プログラムファイルに関する特微量は、公開鍵暗号方式により暗号化されている、
請求項3ないし11の何れか一記載のカプセル化文書構造。

【請求項13】 前記復号化鍵情報は、第三者認証局により署名暗号化されている、
請求項12記載のカプセル化文書構造。

【請求項14】 前記動作プログラムファイルに関する特微量は、秘密鍵暗号方式により暗号化されている、
請求項3ないし11の何れか一記載のカプセル化文書構造。

【請求項15】 前記動作プログラムファイルの改ざん検証を実行する特微量検証プログラムファイルをカプセル化手段によってカプセル化した、
請求項3ないし14の何れか一記載のカプセル化文書構造。

【請求項 16】 請求項 3 ないし 15 の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを格納した、記憶媒体。

【請求項 17】 文書上での表現実体となるコンテンツ情報である文書情報ファイルを取得する文書情報ファイル取得手段と、

コンピュータにより解釈、実行されて、前記文書情報ファイル取得手段により取得された前記文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイルを取得する動作プログラムファイル取得手段と、

前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、

この特徴量算出手段により算出した前記動作プログラムファイルの特徴量を暗号化鍵情報で暗号化し、特徴量保持ファイルに保存する特徴量保持ファイル生成手段と、

前記文書情報ファイルと前記動作プログラムファイルと前記特徴量保持ファイルとを单一の文書としてカプセル化するカプセル化手段と、
を備えるカプセル化文書作成装置。

【請求項 18】 前記文書情報ファイルの特徴量を算出する文書情報特徴量算出手段を備え、

この文書情報特徴量算出手段により算出した前記文書情報ファイルの特徴量も暗号化鍵情報で暗号化し、前記特徴量保持ファイルに保存する、
請求項 17 記載のカプセル化文書作成装置。

【請求項 19】 請求項 3 ないし 15 の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを読み込む読み込み手段と、

この読み込み手段により読み込まれた前記カプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、前記動作プログラムファイルの改ざん検証を実行する改ざん検証手段と、
を備える改ざん検証装置。

【請求項 20】 前記改ざん検証手段は、
前記読み込み手段により読み込まれた前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量を復号化す

る復号化手段と、

前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、

この特徴量算出手段により算出された前記動作プログラムファイルの特徴量と前記復号化手段により復号化された前記動作プログラムファイルの特徴量に基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、

を備える請求項 19 記載の改ざん検証装置。

【請求項 21】 前記改ざん検証手段は、

前記読み込み手段により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、

この特徴量算出手段により算出された前記動作プログラムファイルの特徴量と起動プログラム内の前記動作プログラムファイルの特徴量に基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、

を備える請求項 19 記載の改ざん検証装置。

【請求項 22】 前記改ざん検証手段は、

前記読み込み手段により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、

この特徴量算出手段により算出された前記動作プログラムファイルの特徴量を暗号化する暗号化手段と、

この暗号化手段により暗号化された前記動作プログラムファイルの暗号化特徴量と前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量に基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、

を備える請求項 19 記載の改ざん検証装置。

【請求項 23】 前記改ざん検証手段は、

前記読み込み手段により読み込まれた前記カプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出する特徴量算出手段と、

この特徴量算出手段により算出された前記特徴量検証プログラムファイルの特

微量と起動プログラム内の前記特微量検証プログラムファイルの特微量とに基づいて前記特微量検証プログラムファイルを実行するか否かを判定する判定手段と、

この判定手段により前記特微量検証プログラムファイルを実行すると判定された場合、前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、

を備える請求項19記載の改ざん検証装置。

【請求項24】 コンピュータにインストールされ、

文書上での表現実体となるコンテンツ情報である文書情報ファイルを取得する文書情報ファイル取得機能と、

コンピュータにより解釈、実行されて、前記文書情報ファイル取得機能により取得された前記文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイルを取得する動作プログラムファイル取得機能と、

前記動作プログラムファイルの特微量を算出する特微量算出機能と、

この特微量算出機能により算出した前記動作プログラムファイルの特微量を暗号化鍵情報で暗号化し、特微量保持ファイルに保存する特微量保持ファイル生成機能と、

前記文書情報ファイルと前記動作プログラムファイルと前記特微量保持ファイルとを单一の文書としてカプセル化するカプセル化機能と、

をコンピュータに実行させるカプセル化文書作成処理プログラム。

【請求項25】 前記文書情報ファイルの特微量を算出する文書情報特微量算出機能をコンピュータに実行させ、

この文書情報特微量算出機能により算出した前記文書情報ファイルの特微量も暗号化鍵情報で暗号化し、前記特微量保持ファイルに保存する、

請求項24記載のカプセル化文書作成処理プログラム。

【請求項26】 請求項24または25記載のカプセル化文書作成処理プログラムを記憶する記憶媒体。

【請求項27】 請求項3ないし15の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを読み込む読み込み機能と、

この読み込み機能により読み込まれた前記カプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、前記動作プログラムファイルの改ざん検証を実行する改ざん検証機能と、をコンピュータに実行させる起動プログラム。

【請求項28】 前記改ざん検証機能は、

前記読み込み機能により読み込まれた前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量を復号化する復号化機能と、

前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、

この特徴量算出機能により算出された前記動作プログラムファイルの特徴量と前記復号化機能により復号化された前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、

をコンピュータに実行させる請求項27記載の起動プログラム。

【請求項29】 前記改ざん検証機能は、

前記読み込み機能により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、

この特徴量算出機能により算出された前記動作プログラムファイルの特徴量と起動プログラム内の前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、をコンピュータに実行させる請求項27記載の起動プログラム。

【請求項30】 前記改ざん検証機能は、

前記読み込み機能により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、

この特徴量算出機能により算出された前記動作プログラムファイルの特徴量を暗号化する暗号化機能と、

この暗号化機能により暗号化された前記動作プログラムファイルの暗号化特徴量と前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作

プログラムファイルの暗号化特徴量に基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、
をコンピュータに実行させる請求項27記載の起動プログラム。

【請求項31】 前記改ざん検証機能は、

前記読み込み機能により読み込まれた前記カプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出する特徴量算出機能と、

この特徴量算出機能により算出された前記特徴量検証プログラムファイルの特徴量と起動プログラム内の前記特徴量検証プログラムファイルの特徴量に基づいて前記特徴量検証プログラムファイルを実行するか否かを判定する判定機能と、

この判定機能により前記特徴量検証プログラムファイルを実行すると判定された場合、前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、

をコンピュータに実行させる請求項27記載の起動プログラム。

【請求項32】 請求項27ないし31のいずれか一記載の起動プログラムを記憶する記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、プログラム改ざん検証方法、カプセル化文書構造、記憶媒体、カプセル化文書作成装置、改ざん検証装置、カプセル化文書作成処理プログラム、これを記憶する記憶媒体、起動プログラム及びこれを記憶する記憶媒体に関する。

【0002】

【従来の技術】

現在、コンピュータは各種の情報を表示、作成する道具として一般的である。このような情報は、一般的に「電子文書」と呼ばれている。そして、電子文書は、通常、「文書作成アプリケーションプログラム」と呼ばれるコンピュータ上で動作するプログラムによりデジタル情報として作成され、記憶媒体に保存される。また、作成されたデジタル情報はその情報を読み表示するための「閲覧アプ

リケーションプログラム」と呼ばれるアプリケーションにより表示される。

【0003】

ここで、電子文書を作成・編集するアプリケーションと閲覧するアプリケーションとは同一のプログラムを使用する場合が多い。代表的なものとしてマイクロソフト社のワード（Microsoft Corporationの登録商標）、エクセル（Microsoft Corporationの登録商標）などがある。

【0004】

また、使用者はこの電子文書を扱う場合はこれらのアプリケーションプログラムを予めコンピュータの記憶媒体にインストールしておく必要がある。

【0005】

ところで、電子文書の利用形態を考えると、電子文書を作成する作成者と、閲覧する閲覧者が異なる場合が多い。つまり、閲覧者は、作成者と同じアプリケーションプログラムを保有していないと電子文書を閲覧することができない。そのため、現在の電子文書を扱う場合、閲覧者は作成された電子文書を閲覧するために、電子文書のデジタル情報のフォーマットを解釈できるアプリケーションプログラムを予め用意する必要がある。

【0006】

また、作成者と閲覧者が同じアプリケーションプログラムを保有している場合であっても、作成者と閲覧者とのアプリケーションプログラムのバージョンが異なるために、電子文書の表示フォーマットが乱れたり、表示されなくなる場合がある。

【0007】

そこで、このような問題を解決すべく、本出願人は、特許文献1において、文書のデータ構造として、複数のコンテンツファイルと、それらとそれらの構造を定義した文書構造ファイルと、文書構造ファイルに基づく動作プログラムとを1つのファイルにカプセル化した文書のデータ構造（カプセル化文書）を既に提案している。この特許文献1によれば、電子文書情報に閲覧する動作プログラムをカプセル化することによって、閲覧者は作成者と異なるコンピュータ環境で電子文書を閲覧することが可能になる。

【0008】**【特許文献1】**

特開2003-015941公報

【0009】**【発明が解決しようとする課題】**

しかしながら、このように電子文書内にプログラムを保持させることにより新たな問題が生じる。それは、電子文書内のプログラムが閲覧者の意図しない動作を行う可能性があることである。つまり、電子文書内に悪意のあるプログラムを埋込み、閲覧時に動作させることで閲覧者に被害を与えることである。このままではこのような技術を適用した情報を安全に扱うことができない。特に、現在では、文書をインターネット等を使って配布したりすることが一般に行われているため、コンピュータウィルス等の混入が問題になっている。

【0010】

本発明の目的は、このような問題を解消する新たなデータ構造を提案することである。つまり、コンピュータの動作環境に左右されず、かつ、悪意のあるプログラムの混入を防ぐことを目的とする。

【0011】**【課題を解決するための手段】**

請求項1記載の発明のプログラム改ざん検証方法は、文書上での表現実体となる文書情報ファイルと、当該文書情報ファイルを表現実体化させる動作プログラムファイルとが少なくともカプセル化されているカプセル化文書ファイルにおける前記動作プログラムファイルの改ざん検証処理を情報処理部により実行するプログラム改ざん検証方法であって、前記文書情報ファイルの表現実体化に際して前記カプセル化文書ファイル内の前記動作プログラムファイルの特徴量を算出するステップと、予め保持しておいた前記動作プログラムファイルの暗号化特徴量を復号化するステップと、復号化した前記動作プログラムファイルの特徴量と算出された前記動作プログラムファイルの特徴量とを比較するステップと、特徴量が一致しない場合に、前記動作プログラムファイルによる前記文書情報ファイルの表現実体化を制限するステップと、を具備する。

【0012】

したがって、動作プログラムファイル全体を暗号化処理せずとも、動作プログラムファイルの特微量という小さなデータ（20バイト程度）を暗号化処理するだけで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。これにより、高速にカプセル化文書ファイル内の動作プログラムファイルの改ざん検証が実行できる利便性の高いカプセル化文書ファイルを提供することが可能になる。

【0013】

請求項2記載の発明のプログラム改ざん検証方法は、文書上での表現実体となる文書情報ファイルと、当該文書情報ファイルを表現実体化させる動作プログラムファイルの保存位置を示す位置情報とが少なくともカプセル化されているカプセル化文書ファイルにおける前記動作プログラムファイルの改ざん検証処理を情報処理部により実行するプログラム改ざん検証方法であって、前記文書情報ファイルの表現実体化に際して前記カプセル化文書ファイル内に保持された位置情報に存在する前記動作プログラムファイルの特微量を算出するステップと、予め保持しておいた前記動作プログラムファイルの暗号化特微量を復号化するステップと、復号化した前記動作プログラムファイルの特微量と算出された前記動作プログラムファイルの特微量とを比較するステップと、特微量が一致しない場合に、前記動作プログラムファイルによる前記文書情報ファイルの表現実体化を制限するステップと、を具備する。

【0014】

したがって、動作プログラムファイル全体を暗号化処理せずとも、動作プログラムファイルの特微量という小さなデータ（20バイト程度）を暗号化処理するだけで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。これにより、高速にカプセル化文書ファイル内の動作プログラムファイルの改ざん検証が実行できる利便性の高いカプセル化文書ファイルを提供することが可能になる。

【0015】

請求項3記載の発明のカプセル化文書構造は、各種ファイルで構成されるファ

イル群と、このファイル群を構成する所定のファイルに関する暗号化された特徴量を保持する特徴量保持ファイルと、をカプセル化手段によってカプセル化した。

【0016】

したがって、各種ファイルで構成されるファイル群とファイル群を構成する所定のファイルに関する暗号化された特徴量を保持する特徴量保持ファイルとが一元的に管理されていることにより、カプセル化文書ファイルを配布する際に、所定のファイルの暗号化特徴量を復号化するとともに配布された所定のファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中におけるファイルの改ざん検証が可能になる。

【0017】

請求項4記載の発明のカプセル化文書構造は、文書上での表現実体となるコンテンツ情報である文書情報ファイルと、この文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイルと、この動作プログラムファイルに関する暗号化された特徴量を保持する特徴量保持ファイルと、をカプセル化手段によってカプセル化した。

【0018】

したがって、文書情報ファイルを表現実体化させる動作プログラムファイルが当該文書情報ファイルと一緒にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに配布された動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【0019】

請求項5記載の発明のカプセル化文書構造は、文書上での表現実体となるコンテンツ情報である文書情報ファイルと、この文書情報ファイルを表現実体化させ

る動作プログラムである動作プログラムファイルの保存位置を示す位置情報と、前記動作プログラムファイルに関する暗号化された特微量を保持する特微量保持ファイルと、をカプセル化手段によってカプセル化した。

【0020】

したがって、文書情報ファイルを表現実体化させる動作プログラムファイルの保存位置を示す位置情報が当該文書情報ファイルと一緒にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、特微量保持ファイルに保持されている動作プログラムファイルの暗号化特微量を復号化するとともに所定位置に保存されている動作プログラムファイルの特微量を算出し、復号化した特微量と算出されたファイルの特微量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【0021】

請求項6記載の発明のカプセル化文書構造は、文書上での表現実体となるコンテンツ情報である文書情報ファイルと、この文書情報ファイルを表現実体化させる動作プログラムであり、特微量が外部に保持されている動作プログラムファイルと、をカプセル化手段によってカプセル化した。

【0022】

したがって、文書情報ファイルを表現実体化させる動作プログラムファイルが当該文書情報ファイルと一緒にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、配布された動作プログラムファイルの特微量を算出し、外部に保持されている動作プログラムファイルの特微量と算出されたファイルの特微量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【0023】

請求項7記載の発明のカプセル化文書構造は、文書上での表現実体となるコン

テンツ情報である文書情報ファイルと、この文書情報ファイルを表現実体化させる動作プログラムであり、特微量が外部に保持されている動作プログラムファイルの保存位置を示す位置情報と、をカプセル化手段によってカプセル化した。

【0024】

したがって、文書情報ファイルを表現実体化させる動作プログラムファイルの保存位置を示す位置情報が当該文書情報のファイルと一緒にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、所定位置に保存されている動作プログラムファイルの特微量を算出し、外部に保持されている動作プログラムファイルの特微量と算出されたファイルの特微量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【0025】

請求項8記載の発明は、請求項3ないし5の何れか一記載のカプセル化文書構造において、前記特微量保持ファイルには、前記文書情報ファイルに関する暗号化された特微量も保持されている。

【0026】

したがって、動作プログラムファイルの改ざん検証のみならず、文書情報ファイルの改ざん検証が可能になるので、更に安全に文書を閲覧することが可能になる。

【0027】

請求項9記載の発明は、請求項3ないし5の何れか一記載のカプセル化文書構造において、前記特微量保持ファイルには、前記動作プログラムファイルに関する暗号化された特微量に対応付けられて前記暗号化された特微量を復号化する復号化鍵情報が保持されている。

【0028】

したがって、復号化鍵情報をカプセル化文書ファイル内にカプセル化して閲覧者に配布することによって、閲覧者はカプセル化文書ファイルを取得するだけで動作プログラムファイル等の改ざん検証が可能となる。

【0029】

請求項10記載の発明は、請求項3ないし5の何れか一記載のカプセル化文書構造において、前記特徴量保持ファイルには、前記動作プログラムファイルに関する暗号化された特徴量に対応付けられて前記暗号化された特徴量を復号化する復号化鍵情報の保存位置を示す位置情報を保持している。

【0030】

したがって、復号化鍵情報の保存位置を示す位置情報をカプセル化文書ファイル内にカプセル化して閲覧者に配布することによって、閲覧者はカプセル化文書ファイルを取得するだけで動作プログラムファイル等の改ざん検証が可能となる。

【0031】

請求項11記載の発明は、請求項9または10記載のカプセル化文書構造において、各動作プログラムファイル毎に異なる前記復号化鍵情報が対応付けられている。

【0032】

したがって、例えば1つのベンダーだけでなく複数のベンダーによって複数の動作プログラムファイルが作成されるような場合、閲覧者は、各ベンダーの復号化鍵情報を使用することによって動作プログラムファイルの改ざん検証を行うことが可能になる。これにより、ベンダーごとに作成した動作プログラムファイルに対して、責任を持たせることが可能なカプセル化文書ファイルを提供することが可能になる。

【0033】

請求項12記載の発明は、請求項3ないし11の何れか一記載のカプセル化文書構造において、前記動作プログラムファイルに関する特徴量は、公開鍵暗号方式により暗号化されている。

【0034】

したがって、カプセル化文書ファイルの生成者が所有して公開しない秘密鍵を暗号化鍵とし、秘密鍵とは異なる公開鍵を復号化鍵として閲覧者に公開することにより、公開鍵を有する者だけが動作プログラムファイルに関する特徴量を復号

化することが可能になる。

【0035】

請求項13記載の発明は、請求項12記載のカプセル化文書構造において、前記復号化鍵情報は、第三者認証局により署名暗号化されている。

【0036】

したがって、第三者認証局が作成者側の復号化鍵情報（公開鍵情報）を署名し、カプセル化文書ファイルの信頼性を保証することにより、閲覧者が作成者を既知でなくとも作成者の危険性を判定してカプセル化文書ファイルのセキュリティ機能を保つことが可能になる。

【0037】

請求項14記載の発明は、請求項3ないし11の何れか一記載のカプセル化文書構造において、前記動作プログラムファイルに関する特徴量は、秘密鍵暗号方式により暗号化されている。

【0038】

したがって、暗号化鍵と復号化鍵とが同一の鍵であることにより、暗号化や復号化を高速に実行することが可能になる。

【0039】

請求項15記載の発明は、請求項3ないし14の何れか一記載のカプセル化文書構造において、前記動作プログラムファイルの改ざん検証を実行する特徴量検証プログラムファイルをカプセル化手段によってカプセル化した。

【0040】

したがって、カプセル化文書ファイル内に特徴量検証プログラムファイルを挿入し、起動プログラムが特徴量検証プログラムファイルの改ざん検証と特徴量検証プログラムの起動とを実行することにより、カプセル化文書ファイル内にある複数の動作プログラムファイルの全てに対して改ざん検証を行うことが可能となる。

【0041】

請求項16記載の発明の記憶媒体は、請求項3ないし15の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを格納した。

【0042】

したがって、請求項3ないし15の何れか一記載の発明と同様の作用を奏する。

【0043】

請求項17記載の発明のカプセル化文書作成装置は、文書上での表現実体となるコンテンツ情報である文書情報ファイルを取得する文書情報ファイル取得手段と、コンピュータにより解釈、実行されて、前記文書情報ファイル取得手段により取得された前記文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイルを取得する動作プログラムファイル取得手段と、前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、この特徴量算出手段により算出した前記動作プログラムファイルの特徴量を暗号化鍵情報で暗号化し、特徴量保持ファイルに保存する特徴量保持ファイル生成手段と、前記文書情報ファイルと前記動作プログラムファイルと前記特徴量保持ファイルとを单一の文書としてカプセル化するカプセル化手段と、を備える。

【0044】

したがって、セキュリティ性の高い請求項4記載のファイル構造のカプセル化文書ファイルを簡単に作成することが可能になる。

【0045】

請求項18記載の発明は、請求項17記載のカプセル化文書作成装置において、前記文書情報ファイルの特徴量を算出する文書情報特徴量算出手段を備え、この文書情報特徴量算出手段により算出した前記文書情報ファイルの特徴量も暗号化鍵情報で暗号化し、前記特徴量保持ファイルに保存する。

【0046】

したがって、セキュリティ性の高い請求項8記載のファイル構造のカプセル化文書ファイルを簡単に作成することが可能になる。

【0047】

請求項19記載の発明の改ざん検証装置は、請求項3ないし15の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを読み込む読み込み手段と、この読み込み手段により読み込まれた前記カプセル化文書ファイルに保持された文書

情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、前記動作プログラムファイルの改ざん検証を実行する改ざん検証手段と、を備える。

【0048】

したがって、カプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、動作プログラムファイルの改ざん検証が実行される。これにより、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【0049】

請求項20記載の発明は、請求項19記載の改ざん検証装置において、前記改ざん検証手段は、前記読み込み手段により読み込まれた前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量を復号化する復号化手段と、前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、この特徴量算出手段により算出された前記動作プログラムファイルの特徴量と前記復号化手段により復号化された前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、を備える。

【0050】

したがって、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに配布された動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。

【0051】

請求項21記載の発明は、請求項19記載の改ざん検証装置において、前記改ざん検証手段は、前記読み込み手段により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、この特徴量算出手段により算出された前記動作プログラムファイルの特徴量

と起動プログラム内の前記動作プログラムファイルの特徴量に基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、を備える。
。

【0052】

したがって、配布された動作プログラムファイルの特徴量を算出し、起動プログラム内の特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。

【0053】

請求項22記載の発明は、請求項19記載の改ざん検証装置において、前記改ざん検証手段は、前記読み込み手段により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出手段と、この特徴量算出手段により算出された前記動作プログラムファイルの特徴量を暗号化する暗号化手段と、この暗号化手段により暗号化された前記動作プログラムファイルの暗号化特徴量と前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、を備える。

【0054】

したがって、配布された動作プログラムファイルの特徴量を算出するとともに算出された動作プログラムファイルの特徴量を暗号化し、この暗号化した特徴量と特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。

【0055】

請求項23記載の発明は、請求項19記載の改ざん検証装置において、前記改ざん検証手段は、前記読み込み手段により読み込まれた前記カプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出する特徴量算出手段と、この特徴量算出手段により算出された前記特徴量検証プログラムファイル

の特徴量と起動プログラム内の前記特徴量検証プログラムファイルの特徴量に基づいて前記特徴量検証プログラムファイルを実行するか否かを判定する判定手段と、この判定手段により前記特徴量検証プログラムファイルを実行すると判定された場合、前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行手段と、を備える。

【0056】

したがって、配布されたカプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出し、起動プログラム内の特徴量検証プログラムファイル特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における特徴量検証プログラムファイルの改ざん検証が可能になり、改ざんがなされていない場合に特徴量検証プログラムの起動を実行することにより、カプセル化文書ファイル内にある複数の動作プログラムファイルの全てに対して改ざん検証を行うことが可能となる。

【0057】

請求項24記載の発明のカプセル化文書作成処理プログラムは、コンピュータにインストールされ、文書上での表現実体となるコンテンツ情報である文書情報ファイルを取得する文書情報ファイル取得機能と、コンピュータにより解釈、実行されて、前記文書情報ファイル取得機能により取得された前記文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイルを取得する動作プログラムファイル取得機能と、前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、この特徴量算出機能により算出した前記動作プログラムファイルの特徴量を暗号化鍵情報で暗号化し、特徴量保持ファイルに保存する特徴量保持ファイル生成機能と、前記文書情報ファイルと前記動作プログラムファイルと前記特徴量保持ファイルとを单一の文書としてカプセル化するカプセル化機能と、をコンピュータに実行させる。

【0058】

したがって、セキュリティ性の高い請求項4記載のファイル構造のカプセル化文書ファイルを簡単に作成することが可能になる。

【0059】

請求項25記載の発明は、請求項24記載のカプセル化文書作成処理プログラムにおいて、前記文書情報ファイルの特徴量を算出する文書情報特徴量算出機能をコンピュータに実行させ、この文書情報特徴量算出機能により算出した前記文書情報ファイルの特徴量も暗号化鍵情報で暗号化し、前記特徴量保持ファイルに保存する。

【0060】

したがって、セキュリティ性の高い請求項8記載のファイル構造のカプセル化文書ファイルを簡単に作成することが可能になる。

【0061】

請求項26記載の発明の記憶媒体は、請求項24または25記載のカプセル化文書作成処理プログラムを記憶する。

【0062】

したがって、この記憶媒体に記憶されたカプセル化文書作成処理プログラムをコンピュータに読み取らせることにより、セキュリティ性の高い請求項4または8記載のファイル構造のカプセル化文書ファイルを簡単に作成することが可能になる。

【0063】

請求項27記載の発明の起動プログラムは、請求項3ないし15の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを読み込む読み込み機能と、この読み込み機能により読み込まれた前記カプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、前記動作プログラムファイルの改ざん検証を実行する改ざん検証機能と、をコンピュータに実行させる。

【0064】

したがって、カプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、動作プログラムファイルの改ざん検証が実行される。これにより、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【0065】

請求項28記載の発明は、請求項27記載の起動プログラムにおいて、前記改ざん検証機能は、前記読み込み機能により読み込まれた前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量を復号化する復号化機能と、前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、この特徴量算出機能により算出された前記動作プログラムファイルの特徴量と前記復号化機能により復号化された前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、をコンピュータに実行させる。

【0066】

したがって、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに配布された動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。

【0067】

請求項29記載の発明は、請求項27記載の起動プログラムにおいて、前記改ざん検証機能は、前記読み込み機能により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、この特徴量算出機能により算出された前記動作プログラムファイルの特徴量と起動プログラム内の前記動作プログラムファイルの特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、をコンピュータに実行させる。

【0068】

したがって、配布された動作プログラムファイルの特徴量を算出し、起動プログラム内の特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。

【0069】

請求項30記載の発明は、請求項27記載の起動プログラムにおいて、前記改ざん検証機能は、前記読み込み機能により読み込まれた前記カプセル化文書ファイルに保持された前記動作プログラムファイルの特徴量を算出する特徴量算出機能と、この特徴量算出機能により算出された前記動作プログラムファイルの特徴量を暗号化する暗号化機能と、この暗号化機能により暗号化された前記動作プログラムファイルの暗号化特徴量と前記カプセル化文書ファイルに保持された特徴量保持ファイル内の前記動作プログラムファイルの暗号化特徴量とに基づいて前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、をコンピュータに実行させる。

【0070】

したがって、配布された動作プログラムファイルの特徴量を算出するとともに算出された動作プログラムファイルの特徴量を暗号化し、この暗号化した特徴量と特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になる。

【0071】

請求項31記載の発明は、請求項27記載の起動プログラムにおいて、前記改ざん検証機能は、前記読み込み機能により読み込まれた前記カプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出する特徴量算出機能と、この特徴量算出機能により算出された前記特徴量検証プログラムファイルの特徴量と起動プログラム内の前記特徴量検証プログラムファイルの特徴量とに基づいて前記特徴量検証プログラムファイルを実行するか否かを判定する判定機能と、この判定機能により前記特徴量検証プログラムファイルを実行すると判定された場合、前記動作プログラムファイルの改ざん検証を実行する改ざん検証実行機能と、をコンピュータに実行させる。

【0072】

したがって、配布されたカプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出し、起動プログラム内の特徴量検証プログラムフ

ファイル特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における特徴量検証プログラムファイルの改ざん検証が可能になり、改ざんがなされていない場合に特徴量検証プログラムの起動を実行することにより、カプセル化文書ファイル内にある複数の動作プログラムファイルの全てに対して改ざん検証を行うことが可能となる。

【0073】

請求項32記載の発明の記憶媒体は、請求項27ないし31のいずれか一記載の起動プログラムを記憶する。

【0074】

したがって、この記憶媒体に記憶されたカプセル化文書作成処理プログラムをコンピュータに読み取らせることにより、請求項27ないし31のいずれか一記載の発明と同様の作用を奏する。

【0075】

【発明の実施の形態】

[第一の実施の形態]

本発明の第一の実施の形態を図1ないし図8に基づいて説明する。

【0076】

本発明は、パーソナルコンピュータに代表される各種情報処理装置によって動作する文書のデータ構造（カプセル化文書構造）とその実装形態に関するものであるので、まず、一般的なパーソナルコンピュータで説明する。

【0077】

[1. パーソナルコンピュータ1の構成についての説明]

図1は本実施の形態も適用される一般的又は標準的なパーソナルコンピュータ1のハードウェアの構成図である。パーソナルコンピュータ（以下、コンピュータと略す。）1は、情報処理を行う情報処理部であるC P U（Central Processing Unit）2と、B I O S（Basic Input Output System）等を格納するR O M（Read Only Memory）3と、情報を処理中に一時的に格納するR A M（Random Access Memory）4等の一次記憶装置と、アプリケーションプログラムや処理結果等を保存するH D D（Hard Disk Drive）5等の二次記憶装置と、情報を外部に保

管又は配布し若しくは情報（カプセル化文書ファイル21（図3参照）やアプリケーションプログラム）を外部から入手するための記憶媒体であるリムーバブルメディア6のドライブ6aと、外部の他のコンピュータ1'，…と通信するためのネットワーク7に接続するためのネットワークインタフェース8と、処理経過や処理結果等をユーザに表示するディスプレイ9と、操作者がコンピュータ1に命令や情報等を入力するためのキーボード10やマウス11等の入力装置とから構成され、これらの間のデータ通信をバスコントローラ12が調停して動作している。

【0078】

なお、リムーバブルメディア6としては、フレキシブルディスク、ハードディスク、磁気テープ等のような磁気的な記憶媒体、MOのような光磁気的な記憶媒体、CD、CD-ROM、CD-R、CD-RW、DVD-ROM、DVD-R、DVD-RAM、DVD-RW、DVD+RW等のような光学的な記憶媒体、半導体メモリ等、各種の記憶媒体が適用できる。

【0079】

データ送信は、コンピュータ1のネットワークインタフェース8へとデータを送ることにより、ネットワークインタフェース8がネットワーク7へと信号を出力する。また、ネットワークインタフェース8が受け取った信号については、ネットワークインタフェース8において必要かどうかの判断がなされ、必要なデータであれば取り込み、不必要であれば破棄する、というような処理が行われる。すなわち、あらゆるデータの送受信は、すべてネットワークインタフェース8を経由して行われることになる。

【0080】

一般的に、このようなコンピュータ1ではユーザが電源を投入すると、CPU2はROM3内のBIOSに含まれるローダーというプログラムを起動させ、HDD5からオペレーティングシステム(OS)という当該コンピュータ1のハードウェアとソフトウェアとを管理するプログラムをRAM4に読み込む。OSは起動すると、ユーザの操作に応じてアプリケーションプログラムの起動、情報の読み込み、保存等をサポートする。代表的なOSとしては、Windows(Microso

ft Corporationの登録商標）、UNIX（X/Open, Inc.の登録商標）等が知られている。これらのOS上で走るプログラムをアプリケーションプログラムと呼んでいる。ユーザは、通常、このOSを通してユーザの目的とするアプリケーションプログラムを起動、必要なデータを編集、保存、消去等を行うために記憶装置に記録されているデジタル情報をファイルと言う単位で操作する。つまり、ユーザがコンピュータに対して各種の操作を行う場合はアプリケーションプログラムやデータは全て“ファイル”と言う単位で扱い、それらは記憶装置に保持されている。

【0081】

次に、OSが二次記憶装置等の記憶媒体に保持されているアプリケーションプログラムをユーザの指示により起動する場合について図2を参照して説明する。ユーザがOSに特定のプログラムの起動を指示すると、OSはそのプログラムコードを記憶媒体より記憶装置のハードウェアを使用して読み込み、これをコンピュータ1の一次記憶装置（メモリ）であるRAM4にコードを展開し、展開された特定のアドレスよりCPU2が実行することでプログラムが実行される。通常、このような独立に実行されているプログラムのことを“プロセス”又は“タスク”と称し、記憶媒体に保持された“プログラムコード”と区別している。

【0082】

現在の多くのOSは、このようなプロセス又はタスクを複数同時に走らせるとのできるマルチタスク機能を有するものが一般的である。また、今日のOSはこのような複数のプロセスを同時に走らせるためにプロセス毎に独立してメモリを割り当て動作している。

【0083】

また、このようなプロセス間でデータをやり取りするプロセス間通信のためにメモリ上にメタファイルと言う仮想的なファイルを形成し、ファイルアクセスを介して情報の送受信を行っている。

【0084】

[2. カプセル化文書の説明]

次に、本発明の特長の1つである文書のデータ構造（カプセル化文書構造）の

概要について図3を参照して説明する。このカプセル化文書ファイル21は、コンピュータ1のHDD5に保持されている。本実施の形態のカプセル化文書ファイル21は、文書上での表現実体となる各種のコンテンツや文書構造をファイル化した文書情報ファイル22と、文書情報ファイル22のコンテンツを表現実体化（表示、動作、閲覧等）させる動作プログラムの動作プログラムファイル23と、特微量保持ファイル24とを、单一の文書としてカプセル化手段を用いてカプセル化したものである。これらの情報は、各々一般的なコンピュータ1のOSが管理できる個別のファイル単位の構造となっている。

【0085】

より詳細には、文書情報ファイル22のコンテンツ情報は、静止画像、動画像、音声、テキストファイル等であってコンピュータ1で使用、動作出来るファイルフォーマットに準じてファイル化されている。また、カプセル化手段には、ZIP、LHA等の周知のマルチファイル圧縮方式を使用し、各文書情報ファイル22を閲覧等で表示する場合はこれらのマルチファイル圧縮フォーマットで符号化されているファイルを動的に復号化することで使用する。また、動作プログラムファイル23の動作プログラムは、中間言語コードで記述されている事が望ましい。動作プログラムが中間言語で記述されていれば、この中間言語を解釈実行できるコンパイラまたはインタプリタプログラムがコンピュータにインストールされている状況においてコンピュータの機種依存性が無くなる。このような中間言語としては、java（Sun Microsystemsの登録商標）言語がある。

【0086】

さらに、図3に示すように、特微量保持ファイル24には、各動作プログラムファイル23の特微量を暗号化したものが保存されている。

【0087】

すなわち、従来の技術と異なる点は、各動作プログラムファイル23の特微量が暗号化されて保存されている特微量保持ファイル24をカプセル化文書ファイル21に保持している点である。

【0088】

したがって、文書情報ファイル22を表現実体化させる動作プログラムファイ

ル23が当該文書情報ファイル22と一緒にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、特微量保持ファイル24に保持されている動作プログラムファイル23の暗号化特微量を復号化するとともに配布された動作プログラムファイル23の特微量を算出し、復号化した特微量と算出されたファイルの特微量とを比較することで、カプセル化文書ファイル21の配布途中における動作プログラムファイル23の改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【0089】

[3. コンピュータ1が備える特長的な機能の説明]

次に、コンピュータ1が備える特長的な機能について説明する。

【0090】

[3-1. カプセル化文書作成処理]

コンピュータ1は、内蔵するCPU2がOS上で動作するアプリケーションプログラムに従うことにより、カプセル化文書ファイル21を作成するカプセル化文書作成処理を実行するカプセル化文書作成装置として機能することになる。図4は、CPU2がOS上で動作するアプリケーションプログラムに従うことにより実現されるカプセル化文書作成処理の流れを示すフローチャートである。

【0091】

図4に示すように、まず、ユーザの操作に応じて文書上での表現実体となるコンテンツ（閲覧者へ伝えたい文書内容）である文書情報ファイル22を生成する（ステップS1：文書情報ファイル取得手段）。このような文書情報ファイル22の生成は、一般のワードプロセッシングソフト等により実現可能である。次いで、文書情報ファイル22内のコンテンツを表現実体化（表示、動作、閲覧等）させる動作プログラムファイル23を生成する（ステップS2：動作プログラムファイル取得手段）。

【0092】

続くステップS3においては、ステップS2で生成した動作プログラムファイル23の特微量を算出する。ここに、特微量算出手段の機能が実行される。動作

プログラムファイル23の特徴量とは、動作プログラムファイル23に対する電子指紋である。このような特徴量の算出方法としては、SHA1 (Secure-Hash-Algorithm) などが挙げられる。SHA1では、動作プログラムとなる任意の長さのデータブロックを20バイトのシーケンスで圧縮する。実際の指紋と同様に2つの異なる動作プログラムの特徴量は、必ず異なることを期待されるが、特徴量の値の種類は有限であるために異なる動作プログラムにおいても同じ特徴量が算出される可能性がある。しかし、特徴量は2160種類という莫大な数へと変換できるため、異なる動作プログラムから同一の特徴量を生成する可能性を確率的に無視することができる。SHA1の基本的な特性として、動作プログラムを1ビットでも変更すると動作プログラムの特徴量も変更されることと、特徴量の偽造を試みても元の特徴量と同じ特徴量を持つ偽造メッセージを生成できないことの2点が挙げられる。この特性により、動作プログラムと動作プログラムの特徴量が一対一の関係となることが立証される。SHA1以外の特徴量の算出方法としては、Massachusetts Institute of TechnologyのRonald Rivest氏が発明したMD5なども挙げられる。なお、動作プログラムファイル23の特徴量の算出には、SHA1、MD5以外の手法を使用しても良い。また、特徴量算出の実行手段の一例としては、動作プログラムがjava言語で記載されているときには、Sun Microsystems社から提供されているjavaのsecurityパッケージにあるプログラムを使用することによって容易に特徴量を算出できる。

【0093】

次いで、秘密鍵・公開鍵を生成し（ステップS4）、生成した秘密鍵で動作プログラムファイル23の特徴量を暗号化する（ステップS5）。秘密鍵を利用した暗号化には、RSAやDSA (Digital Signature Algorithm) などを利用する。RSAの暗号アルゴリズムは大きな数値の素因数分解を実行することが困難であるという事実に依存したものであり、2000ビット以上の係数を持つ鍵であれば安全であると一般的に知られている。RSA、DSAなどは、様々な企業から提供されているため、簡単に使用することが可能である。なお、暗号化に使用する秘密鍵・公開鍵を生成する代わりに、作成者のコンピュータ内に予め保持された秘密鍵・公開鍵を使用するようにしても良い。

【0094】

すなわち、本実施の形態においては、公開鍵暗号方式により動作プログラムファイル23の特徴量を暗号化するものである。これにより、カプセル化文書ファイル21の生成者が所有して公開しない秘密鍵を暗号化鍵とし、秘密鍵とは異なる公開鍵を復号化鍵として閲覧者に公開することにより、公開鍵を有する者だけが動作プログラムファイル23に関する特徴量を復号化することが可能になる。

【0095】

そして、このように秘密鍵で暗号化された動作プログラムファイル23の特徴量を特徴量保持ファイル24に保存した後（ステップS6：特徴量保持ファイル生成手段）、文書情報ファイル22と動作プログラムファイル23と特徴量保持ファイル24とを单一の文書としてカプセル化手段を用いてカプセル化したカプセル化文書ファイル21を作成する（ステップS7）。なお、暗号化された動作プログラムファイル23の特徴量を特徴量保持ファイル24に保存する際には、動作プログラムファイル23と暗号化された動作プログラムファイルの特徴量との対応が付くようにしておく。暗号化された動作プログラムファイル23の特徴量を動作プログラムファイル23に対応付けてXMLで表記した例を図5に示す。図5に示すように、特徴量保持ファイル24には、動作プログラムタグ内の属性情報として、暗号化された動作プログラムファイルの特徴量が保存されている。また、図5に示すように、特徴量保持ファイル24の特徴量算出情報タグ内の属性情報であるアルゴリズムには、作成者が動作プログラムファイル23の特徴量を算出した際に使用した特徴量算出アルゴリズムが記載されている。

【0096】

以上のようにして作成されたカプセル化文書ファイル21は、動作プログラムファイル23の特徴量の暗号化に使用された秘密鍵と対になる公開鍵とともに、ネットワーク7を介して所定のコンピュータ1に対して送信されて配布されることになる。

【0097】

[3-2. 改ざん検証処理]

コンピュータ1は、内蔵するCPU2がOS内にあるShellプログラムが関連

付けされているカプセル化文書起動プログラム（以下、起動プログラムという。）に従うことにより、動作プログラムファイル23の改ざん検証処理を実行する改ざん検証装置として機能することになる。ここでは、図3に示すようなカプセル化文書ファイル21が公開鍵とともに別のコンピュータ1（カプセル化文書作成装置）から配布されたものとして説明する。

【0098】

閲覧者がキーボード10やマウス11等の入力装置を介してカプセル化文書ファイル21を選択した際に、OS内にあるShellプログラムが拡張子等でカプセル化文書ファイル21と判断した場合には、起動プログラムが起動する。起動プログラムは、選択されたカプセル化文書ファイル21を読み込み、カプセル化文書ファイル21内にある動作プログラムファイル23の改ざん検証をする。

【0099】

図6は、起動プログラムによる改ざん検証処理の流れを示すフローチャートである。図6に示すように、まず、配布されたカプセル化文書ファイル21と公開鍵を取得して解凍すると（ステップS11：読み込み手段）、取得した公開鍵を使用してカプセル化文書ファイル21内にある暗号化された動作プログラムファイル23の特微量を復号化する（ステップS12：復号化手段）。

【0100】

次いで、ステップS11で取得したカプセル化文書ファイル21内の動作プログラムファイル23の特微量を算出する（ステップS13：特微量算出手段）。動作プログラムファイル23の特微量の算出は、カプセル化文書作成装置での処理と同様に、SHA1、MD5の手法を使用しても良いし、javaのsecurityパッケージにあるプログラムを使用しても良いが、原則的には作成者側と閲覧者側との特微量算出アルゴリズムを一致させることが必要である。前述したように、特微量保持ファイル24の特微量算出情報タグ内の属性情報であるアルゴリズムには、作成者が動作プログラムファイル23の特微量を算出した際に使用した特微量算出アルゴリズムが記載されているので（図5参照）、この特微量算出アルゴリズム情報に基づいて動作プログラムファイル23の特微量の算出を行えば良い。なお、作成者側と閲覧者側との特微量算出アルゴリズムが対応していれば、必

ずしも同一の特微量算出アルゴリズムで動作プログラムファイル23の特微量を算出しなくても良い。

【0101】

次いで、ステップS14に進み、配布されたカプセル化文書ファイル21内の暗号化された動作プログラムファイル23の特微量を復号化した値と閲覧者側で動作プログラムファイル23の特微量を算出した値とを比較し、動作プログラムファイル23の改ざん検証を実行する。ここに、改ざん検証実行手段の機能が実行される。ここで、同一の特微量算出アルゴリズムを使用して同一な動作プログラムファイル23の特微量を算出することにより、カプセル化文書ファイル21内の動作プログラムファイル23に改ざんがなければ、配布されたカプセル化文書ファイル21内の暗号化された動作プログラムファイル23の特微量を復号化した値と閲覧者側で動作プログラムファイル23の特微量を算出した値は一致することになる。したがって、2つの特微量を比較することにより、動作プログラムファイル23の改ざんを検証することができる。

【0102】

つまり、ステップS12～S14において、改ざん検証手段の機能が実行される。

【0103】

動作プログラムファイル23の改ざん検証を行った結果、2つの特微量が一致していれば、すなわち動作プログラムファイル23が改ざんされていなければ（ステップS15のN）、動作プログラムファイル23に記載された署名情報をディスプレイ9に表示し（ステップS16）、表示された署名者が信用できるかを閲覧者に判断させる。

【0104】

信用できる署名者である旨がキーボード10やマウス11等の入力装置を介して閲覧者により入力された場合には（ステップS17のY）、動作プログラムファイル23の動作プログラムを実行してディスプレイ9上にカプセル化文書ファイル21内の文書情報ファイル22を表示する（ステップS18）。

【0105】

一方、動作プログラムファイル23の改ざん検証を行った結果、2つの特徴量が一致しなければ、すなわち動作プログラムファイル23が改ざんされている場合（ステップS15のY）、信用できる署名者でない旨がキーボード10やマウス11等の入力装置を介して閲覧者により入力された場合には（ステップS17のN）、動作プログラムファイル23の動作プログラムを実行せずに、不正なプログラムファイルであることを報知する不正報知処理を実行する（ステップS19）。不正報知処理としては、例えば、カプセル化文書ファイル21内の動作プログラムファイル23が配布途中で改ざんされたことを通知するダイアログボックスをディスプレイ9上に表示することが考えられる。また、不正なプログラムファイルである旨を表示するのみに留まらず、カプセル化文書ファイル21の動作プログラムファイル23を消去するかどうかユーザに促しても良い。

【0106】

通常、特徴量情報は20バイトの情報量で生成されるが、改ざん検証を行う動作プログラムファイル23の危険性に応じて、特徴量情報の情報量を変化させても良い。動作プログラムファイル23の改ざん検証を行う際に使用する動作プログラムファイル23の特徴量情報の情報量は、小さい方が高速に動作プログラムファイル23の改ざん検証を実行できるが、あまりにも小さすぎると特徴量のバリエーションが乏しくなり改ざんされる危険性が増加する。したがって、危険性の低い動作プログラムファイル23は小さな情報量となるように特徴量情報を算出し、危険性の高い動作プログラムファイル23は大きな情報量となるように特徴量情報を算出しても良い。この際、閲覧者側へ動作プログラムファイル23の改ざん検証がどれだけ安全に機能しているかを通知するために、改ざん検証に使用された特徴量情報の情報量の大きさを閲覧者側へ表示させる必要がある。そこで、特徴量保持ファイル24内に保持される暗号化された動作プログラムファイル23の特徴量を復号化した値又は閲覧者側で動作プログラムファイル23の特徴量を算出した値を、ディスプレイ9上に表示するようにしても良い。このように特徴量情報を閲覧者側のコンピュータ1のディスプレイ9へ表示するための特徴量情報表示プログラムファイルをカプセル化文書ファイル21内にカプセル化することによって、閲覧者側へ改ざん検証機能の安全性を通知することのできる

カプセル化文書ファイルを提供することができる。

【0107】

このように本実施の形態によれば、カプセル化文書作成装置と改ざん検証装置とを備え、動作プログラムファイル23全体を暗号化処理せずとも、動作プログラムファイル23の特徴量という20バイト程度の小さなデータを暗号化処理するだけで、カプセル化文書ファイル21の配布途中における動作プログラムファイル23の改ざん検証ができる。これにより、高速にカプセル化文書ファイル21内の動作プログラムファイル23の改ざん検証が実行できる利便性の高いカプセル化文書ファイル21を提供することができる。

【0108】

なお、起動プログラムは、OS内にあるShellプログラムで起動するものに限るものではなく、Shellプログラムがこの様な機能を有しても良い。

【0109】

なお、動作プログラムファイル23を暗号化する秘密鍵を複数用意し、動作プログラムファイル23の動作権限に対応させて復号化する公開鍵を変更するようにも良い。動作プログラムの実行内容によって動作プログラムファイル23の危険性は変化することが考えられる。例えば、動作プログラムファイル23が文書情報ファイル22を表示するだけならば危険性は少ないが、動作プログラムファイル23が文書情報ファイル22を編集する機能を追加する場合には動作プログラムファイル23の危険性が高くなる。そこで、閲覧者側のコンピュータ1には予め動作プログラムファイル23の処理を制限する動作制限情報を設定しておき、動作制限情報に対応させて復号化する公開鍵を変更することにより、危険性の高い動作プログラムファイル23を実行させないようにすることができる。

【0110】

より具体的には、図7に示すように、ファイルの読み書き、ネットワークの送受信等を許可（○で示す）、非許可（×で示す）の動作権限のモードに応じて復号化する公開鍵を用意し、動作プログラムファイル23を実行する際に必要な公開鍵の動作権限情報をディスプレイ9を通じて閲覧者に表示することで、閲覧者

に許可をもらってそのモードの動作権限で動作プログラムファイル23を起動しても良い。例えば図7に示す動作権限モードがBであれば、カプセル化文書ファイル21内のファイルを読み込むプログラムだけを実行させる。同様にして動作権限モードがCであれば、カプセル化文書ファイル21内のファイルを読み込むプログラム及びコンピュータ1内のファイルを読み込むプログラムだけが実行される。

【0111】

動作プログラムの動作権限を制限する方法は、上述した方法に限るものではない。例えば、動作プログラムに中間コードを使用する場合はこれを解釈実行するのにインタプリタが必要になりこのインタプリタを通してコンピュータの入出力を行うので簡単に動作権限を制限できる。また、動作プログラムがネイティブなコードの場合は実行に先立って実行コードを検出し、権限外の動作を制限すれば良い。また、このような動作権限の制限機能は現在の標準的なオペレーティングシステムに備わっているのでこれを利用しても良い。

【0112】

以上により、閲覧者側の動作制限情報に応じて動作プログラムファイル23を実行するカプセル化文書ファイル21が提供できる。

【0113】

また、動作プログラムファイル23の1つとして動作権限情報通知プログラムを追加し、閲覧者側の動作権限情報を作成者へ知らせるようにしても良い。動作権限情報通知プログラムは、閲覧者側のコンピュータ1のディスプレイ9上に動作権限情報を作成者へ通知しても良いかを判定させるダイアログボックスを表示させる。閲覧者が動作権限情報の通知を許諾すれば、動作権限情報通知プログラムを実行して閲覧者側のコンピュータ1内に設定されている動作権限情報を作成者側へ通知する。作成者は、閲覧者側から通知された動作権限情報を見て、閲覧者側の動作権限情報によって以前に配布したカプセル化文書ファイル21内にある文書情報ファイル22が表示されないと判断したときには、閲覧者側の動作権限情報に応じて動作プログラムファイル23を変更したカプセル化文書ファイル21を再度、閲覧者へ配布しても良い。

【0114】

これにより、動作プログラムファイル23の閲覧者側の動作権限情報によって制限されるときには、作成者へカプセル化文書ファイル21内の動作プログラムファイル23が閲覧者側で起動されないことを通知するカプセル化文書ファイル21を提供することができる。

【0115】

なお、本実施の形態においては、暗号化された動作プログラムファイル23の特徴量を復号化したものと閲覧者側で動作プログラムファイル23の特徴量を算出したものを比較し、動作プログラムファイル23の改ざん検証を実行するようにしたが、これに限るものではなく、暗号化された動作プログラムファイル23の特徴量と閲覧者側で算出した動作プログラムファイル23の特徴量を暗号化したもの（暗号化手段）とを比較し、動作プログラムファイル23の改ざん検証を実行するようにしても良い。

【0116】

[4. 本実施の形態の変形例]

[4-1. 第1の変形例]

本実施の形態においてはカプセル化文書ファイル21を公開鍵とともに配布するようにしたが、公開鍵をカプセル化文書ファイル21内にカプセル化するようにも良い。秘密鍵により暗号化された動作プログラムファイル23の特徴量と、この秘密鍵と対になる公開鍵の情報である公開鍵情報を動作プログラムファイル23に対応付けてXMLで表記した例を図8に示す。図8に示すように、特徴量保持ファイル24には、動作プログラムタグ内の属性情報として、秘密鍵により暗号化された動作プログラムファイル23の特徴量と、この秘密鍵と対になる公開鍵の情報である公開鍵情報を保存されている。

【0117】

ところで、特徴量保持ファイル24の公開鍵情報としては、公開鍵そのものに限るものではなく、公開鍵の位置情報であっても良い。例えば、公開鍵が保持されているインターネット上の位置情報（URL（Uniform Resource Locator））を記述しても良い（図8に示す“動作プログラム3”の公開鍵情報）。この場合

は、インターネットにコンピュータ1が接続されていることが前提になる。また、インターネット上に公開された公開鍵情報は、閲覧者が接続した際に閲覧者のコンピュータ1の記憶媒体（RAM4やHDD5等）へ保存されるようにしても良い。このようにすることで、カプセル化文書ファイル21内に公開鍵情報が保存されていない場合は、閲覧者のコンピュータの記憶媒体（RAM4やHDD5等）に保存された公開鍵情報を代わりに使用することができる。

【0118】

このように公開鍵（公開鍵の位置情報）をカプセル化文書ファイル21内にカプセル化して閲覧者に配布することによって、閲覧者は改ざん検証装置を用いてカプセル化文書ファイル21を取得するだけで動作プログラムファイル23の改ざん検証が可能となる。

【0119】

このような第1の変形例の具体例としては、各ベンダーが作成した動作プログラムファイル23の特徴量に対して秘密鍵により暗号化を行い、復号化するための公開鍵情報を特徴量保持ファイル24に保存するような場合が考えられる。図8に示すように、例えば動作プログラム1はベンダーA社で、動作プログラム2はベンダーB社で作成するような場合である。このような事態が生じるのは、現在のプログラム開発は、一人で全プログラムを作成する例は少なく、多人数で協力し合いながらプログラムを作成することが一般的であり、大規模なプログラムとなると1つのベンダーだけでなく複数のベンダーによって複数の動作プログラムファイルが作成されるためである。つまり、カプセル化文書ファイル21内にカプセル化される動作プログラムファイル23も、複数のベンダーによって作成されることが予想される。

【0120】

閲覧者は、特徴量保持ファイル24に保存されている各ベンダーの公開鍵情報を使用することによって動作プログラムファイル23の改ざん検証を行い、検証の際、動作プログラムファイル23の改ざんがなければ、動作プログラムファイル23を作成したベンダーの署名情報を表示し、動作プログラムファイル23を実行する。

【0121】

このように各動作プログラムファイル23毎に異なる公開鍵情報が対応付けられることにより、ベンダーごとに作成した動作プログラムファイル23に対して、責任を持たせることが可能なカプセル化文書ファイル21を提供することができる。

【0122】

[4-2. 第2の変形例]

本実施の形態においては、文書情報ファイル22と動作プログラムファイル23と特微量保持ファイル24とを单一の文書としてカプセル化手段を用いてカプセル化したカプセル化文書ファイル21を配布するようにしたが、カプセル化文書ファイル21内に動作プログラムファイル23を必ずしも保持しなくとも良い。このような場合、特微量保持ファイル24において“動作プログラムファイルと暗号化された動作プログラムファイルの特微量”の対応が付けられるように位置情報を追加するなどの工夫が必要となる。位置情報を追加して動作プログラムの特微量情報を保存した特微量保持ファイル24のファイルフォーマット例を図9に示す。図9に示すように、動作プログラムタグ内の属性情報として記載された位置情報としては、動作プログラムが保存されているインターネット上の位置情報（URL（Uniform Resource Locator））を記述しても良い。この場合は、インターネットにコンピュータ1が接続されていることが前提になる。図9の特微量には、動作プログラムタグ内の属性情報として記載された位置情報に位置する動作プログラムファイルの特微量を作成者の秘密鍵で暗号化した結果が記載されている。図9に示すようなファイルフォーマットにすることによって、動作プログラムファイルが物理的に単一ファイルにカプセル化されていなくとも、動作プログラムファイル23の改ざん検証が可能となる。

【0123】

したがって、文書情報ファイル22を表現実体化させる動作プログラムファイル23の保存位置を示す位置情報が当該文書情報ファイル22と一緒にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、特微量保持ファイル24に保持されている動作プロ

グラムファイル23の暗号化特徴量を復号化するとともに所定位置に保存されている動作プログラムファイル23の特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイル21の配布途中における動作プログラムファイル23の改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【0124】

なお、動作プログラムファイルの一部のみを動作プログラムファイル23として文書情報ファイル22や特徴量保持ファイル24とともにカプセル化し、残りの動作プログラムファイルをインターネット上の所定の位置に保存するようにしても良い。

【0125】

[第二の実施の形態]

本発明の第二の実施の形態を図10ないし図12に基づいて説明する。なお、本発明の第一の実施の形態において説明した部分と同一部分については同一符号を用い、説明も省略する。

【0126】

[1. カプセル化文書の説明]

本発明の特長の1つである文書のデータ構造（カプセル化文書構造）の概要について図10を参照して説明する。このカプセル化文書ファイル21は、コンピュータ1のHDD5に保持されている。本実施の形態のカプセル化文書ファイル21は、文書上での表現実体となる各種のコンテンツや文書構造をファイル化した文書情報ファイル22と、文書情報ファイル22を表現実体化させる動作プログラムの動作プログラムファイル23と、特徴量保持ファイル24とを、单一の文書としてカプセル化手段を用いてカプセル化したものである。これらの情報は、各々一般的なコンピュータ1のOSが管理できる個別のファイル単位の構造となっている。

【0127】

より詳細には、文書情報ファイル22のコンテンツ情報は、静止画像、動画像、音声、テキストファイル等であってコンピュータ1で使用、動作出来るファイ

ルフォーマットに準じてファイル化されている。また、カプセル化手段には、ZIP、LHA等の周知のマルチファイル圧縮方式を使用し、各文書情報ファイル22を閲覧等で表示する場合はこれらのマルチファイル圧縮フォーマットで符号化されているファイルを動的に復号化することで使用する。また、動作プログラムファイル23の動作プログラムは、中間言語コードで記述されている事が望ましい。動作プログラムが中間言語で記述されていれば、この中間言語を解釈実行できるコンパイラまたはインタプリタプログラムがコンピュータにインストールされている状況においてコンピュータの機種依存性が無くなる。このような中間言語としては、java（Sun Microsystemsの登録商標）言語がある。

【0128】

さらに、図10に示すように、特微量保持ファイル24には、各動作プログラムファイル23の特微量を暗号化したものと、各文書情報ファイル22の特微量を暗号化したものとが保存されている。

【0129】

すなわち、従来の技術と異なる点は、各動作プログラムファイル23の特微量と各文書情報ファイル22の特微量とが暗号化されて保存されている特微量保持ファイル24をカプセル化文書ファイル21に保持している点である。

【0130】

[2. コンピュータ1が備える特長的な機能の説明]

次に、コンピュータ1が備える特長的な機能について説明する。

【0131】

[2-1. カプセル化文書作成処理]

コンピュータ1は、内蔵するCPU2がOS上で動作するアプリケーションプログラムに従うことにより、カプセル化文書ファイル21を作成するカプセル化文書作成処理を実行するカプセル化文書作成装置として機能することになる。図11は、CPU2がOS上で動作するアプリケーションプログラムに従うことにより実現されるカプセル化文書作成処理の流れを示すフローチャートである。

【0132】

図11に示すように、まず、ユーザの操作に応じて文書上での表現実体となる

コンテンツ（閲覧者へ伝えたい文書内容）である文書情報ファイル22を生成する（ステップS21：文書情報ファイル取得手段）。このような文書情報ファイル22の生成は、一般的のワードプロセッシングソフト等により実現可能である。次いで、文書情報ファイル22内のコンテンツを表現実体化（表示、動作、閲覧等）させる動作プログラムファイル23を生成する（ステップS22：動作プログラムファイル取得手段）。

【0133】

続くステップS23においては、ステップS22で生成した動作プログラムファイル23の特徴量を算出する。ここに、特徴量算出手段の機能が実行される。動作プログラムファイル23の特徴量とは、動作プログラムファイル23に対する電子指紋である。このような特徴量の算出方法としては、SHA1（Secure-Hash-Algorithm）などが挙げられる。SHA1では、動作プログラムとなる任意の長さのデータブロックを20バイトのシーケンスで圧縮する。実際の指紋と同様に2つの異なる動作プログラムの特徴量は、必ず異なることを期待されるが、特徴量の値の種類は有限であるために異なる動作プログラムにおいても同じ特徴量が算出される可能性がある。しかし、特徴量は2160種類という莫大な数へと変換できるため、異なる動作プログラムから同一の特徴量を生成する可能性を確率的に無視することができる。SHA1の基本的な特性として、動作プログラムを1ビットでも変更すると動作プログラムの特徴量も変更されること、特徴量の偽造を試みても元の特徴量と同じ特徴量を持つ偽造メッセージを生成できないことの2点が挙げられる。この特性により、動作プログラムと動作プログラムの特徴量が一対一の関係となることが立証される。SHA1以外の特徴量の算出方法としては、Massachusetts Institute of TechnologyのRonald Rivest氏が発明したMD5なども挙げられる。なお、動作プログラムファイル23の特徴量の算出には、SHA1、MD5以外の手法を使用しても良い。また、特徴量算出の実行手段の一例としては、動作プログラムがjava言語で記載されているときには、Sun Microsystems社から提供されているjavaのsecurityパッケージにあるプログラムを使用することによって容易に特徴量を算出できる。

【0134】

また、ステップS21で生成した文書情報ファイル22についても特徴量を算出する（ステップS24：文書情報特徴量算出手段）。文書情報ファイル22の特徴量算出は、動作プログラムファイル23の特徴量算出方法と同様な方法で算出すれば良い。

【0135】

次いで、秘密鍵・公開鍵を生成し（ステップS25）、生成した秘密鍵で動作プログラムファイル23の特徴量及び文書情報ファイル22の特徴量を暗号化する（ステップS26）。秘密鍵を利用した暗号化には、RSAやDSA（Digital Signature Algorithm）などを利用する。RSAの暗号アルゴリズムは大きな数値の素因数分解を実行することが困難であるという事実に依存したものであり、2000ビット以上の係数を持つ鍵であれば安全であると一般的に知られている。RSA、DSAなどは、様々な企業から提供されているため、簡単に使用することが可能である。なお、暗号化に使用する秘密鍵・公開鍵を生成する代わりに、作成者のコンピュータ内に予め保持された秘密鍵・公開鍵を使用するようにしても良い。すなわち、本実施の形態においては、公開鍵暗号方式により動作プログラムファイル23の特徴量及び文書情報ファイル22の特徴量を暗号化するものである。

【0136】

そして、このように秘密鍵で暗号化された動作プログラムファイル23の特徴量及び文書情報ファイル22の特徴量を特徴量保持ファイル24に保存した後（ステップS27：特徴量保持ファイル生成手段）、文書情報ファイル22と動作プログラムファイル23と特徴量保持ファイル24とを单一の文書としてカプセル化手段を用いてカプセル化したカプセル化文書ファイル21を作成する（ステップS28）。なお、暗号化された動作プログラムファイル23の特徴量及び文書情報ファイル22の特徴量を特徴量保持ファイル24に保存する際には、動作プログラムファイル23と暗号化された動作プログラムファイルの特徴量との対応、文書情報ファイル22と文書情報ファイル22の特徴量との対応が付くようにしておく。

【0137】

以上のようにして作成されたカプセル化文書ファイル21は、動作プログラムファイル23の特徴量及び文書情報ファイル22の特徴量の暗号化に使用された秘密鍵と対になる公開鍵とともに、ネットワーク7を介して所定のコンピュータ1に対して送信されて配布されることになる。

【0138】

[2-2. 改ざん検証処理]

コンピュータ1は、内蔵するCPU2がOS内にあるShellプログラムが関連付けされている起動プログラムに従うことにより、動作プログラムファイル23の改ざん検証処理を実行する改ざん検証装置として機能することになる。ここでは、図10に示すようなカプセル化文書ファイル21が公開鍵とともに別のコンピュータ1（カプセル化文書作成装置）から配布されたものとして説明する。

【0139】

閲覧者がキーボード10やマウス11等の入力装置を介してカプセル化文書ファイル21を選択した際に、OS内にあるShellプログラムが拡張子等でカプセル化文書ファイル21と判断した場合には、起動プログラムが起動する。起動プログラムは、選択されたカプセル化文書ファイル21を読み込み、カプセル化文書ファイル21内にある動作プログラムファイル23の改ざん検証をする。

【0140】

図12は、起動プログラムによる改ざん検証処理の流れを示すフローチャートである。図12に示すように、まず、配布されたカプセル化文書ファイル21と公開鍵を取得して解凍すると（ステップS31：読み込み手段）、取得した公開鍵を使用してカプセル化文書ファイル21内にある暗号化された動作プログラムファイル23の特徴量を復号化する（ステップS32：復号化手段）。

【0141】

次いで、ステップS31で取得したカプセル化文書ファイル21内の動作プログラムファイル23の特徴量を算出する（ステップS33：特徴量算出手段）。動作プログラムファイル23の特徴量の算出は、カプセル化文書作成装置での処理と同様に、SHA1、MD5の手法を使用しても良いし、javaのsecurityパッケージにあるプログラムを使用しても良いが、原則的には作成者側と閲覧者側と

の特微量算出アルゴリズムを一致させることが必要である。前述したように、特微量保持ファイル24の特微量算出情報タグ内の属性情報であるアルゴリズムには、作成者が動作プログラムファイル23の特微量を算出した際に使用した特微量算出アルゴリズムが記載されている（図5参照）、この特微量算出アルゴリズム情報に基づいて動作プログラムファイル23の特微量の算出を行えば良い。なお、作成者側と閲覧者側との特微量算出アルゴリズムが対応していれば、必ずしも同一の特微量算出アルゴリズムで動作プログラムファイル23の特微量を算出しなくても良い。

【0142】

次いで、ステップS34に進み、配布されたカプセル化文書ファイル21内の暗号化された動作プログラムファイル23の特微量を復号化した値と閲覧者側で動作プログラムファイル23の特微量を算出した値とを比較し、動作プログラムファイル23の改ざん検証を実行する。ここに、改ざん検証実行手段の機能が実行される。ここで、同一の特微量算出アルゴリズムを使用して同一な動作プログラムファイル23の特微量を算出することにより、カプセル化文書ファイル21内の動作プログラムファイル23に改ざんがなければ、配布されたカプセル化文書ファイル21内の暗号化された動作プログラムファイル23の特微量を復号化した値と閲覧者側で動作プログラムファイル23の特微量を算出した値は一致することになる。したがって、2つの特微量を比較することにより、動作プログラムファイル23の改ざんを検証することができる。

【0143】

つまり、ステップS32～S34において、改ざん検証手段の機能が実行される。

【0144】

動作プログラムファイル23の改ざん検証を行った結果、2つの特微量が一致していれば、すなわち動作プログラムファイル23が改ざんされていなければ（ステップS35のN）、動作プログラムファイル23に記載された署名情報をディスプレイ9に表示し（ステップS36）、表示された署名者が信用できるかを閲覧者に判断させる。

【0145】

信用できる署名者である旨がキーボード10やマウス11等の入力装置を介して閲覧者により入力された場合には（ステップS37のY）、動作プログラムファイル23の文書情報ファイル検証プログラムを起動させる（ステップS38）。

【0146】

文書情報ファイル検証プログラムは、取得した公開鍵により暗号化された文書情報ファイル22の特徴量を復号化し（ステップS39：復号化手段）、文書情報ファイル22の特徴量を復号化した値と閲覧者側で文書情報ファイル22の特徴量を算出した値とを比較し、文書情報ファイル22の改ざん検証を実行する（ステップS40）。つまり、ステップS38～S40において、改ざん検証手段の機能が実行される。

【0147】

文書情報ファイル22の改ざん検証を行った結果、2つの特徴量が一致していれば、すなわち文書情報ファイル22が改ざんされていなければ（ステップS41のN）、動作プログラムファイル23の動作プログラム（文書閲覧プログラム）を起動して文書情報ファイル22をディスプレイ9に表示する（ステップS42）。

【0148】

一方、動作プログラムファイル23が改ざんされている場合（ステップS35のY）、信用できる署名者でない旨がキーボード10やマウス11等の入力装置を介して閲覧者により入力された場合（ステップS37のN）、文書情報ファイル22が改ざんされている場合（ステップS41のY）、不正なプログラムファイルであることを報知する不正報知処理を実行する（ステップS43）。不正報知処理としては、例えば、カプセル化文書ファイル21内の動作プログラムファイル23や文書情報ファイル22が配布途中で改ざんされたことを通知するダイアログボックスをディスプレイ9上に表示することが考えられる。また、改ざんされたことを作成者側にも通知し、新たにカプセル化文書ファイル21の配布を要求しても良い。

【0149】

このように本実施の形態によれば、カプセル化文書作成装置と改ざん検証装置とを備え、動作プログラムファイル23全体及び文書情報ファイル22全体を暗号化処理せずとも、動作プログラムファイル23の特徴量及び文書情報ファイル22の特徴量という20バイト程度の小さなデータを暗号化処理するだけで、カプセル化文書ファイル21の配布途中における動作プログラムファイル23及び文書情報ファイル22の改ざん検証ができる。これにより、高速にカプセル化文書ファイル21内の動作プログラムファイル23及び文書情報ファイル22の改ざん検証が実行できる利便性の高いカプセル化文書ファイル21を提供することができる。すなわち、動作プログラムファイル23の改ざん検証のみならず、文書情報ファイル22の改ざん検証が可能になるので、更に安全に文書を閲覧することが可能になる。

【0150】

なお、起動プログラムは、OS内にあるShellプログラムで起動するものに限るものではなく、Shellプログラムがこの様な機能を有しても良い。

【0151】

[第三の実施の形態]

本発明の第三の実施の形態を図13または図14に基づいて説明する。なお、本発明の第一の実施の形態または第二の実施の形態において説明した部分と同一部分については同一符号を用い、説明も省略する。

【0152】

第一の実施の形態または第二の実施の形態によれば、カプセル化文書ファイル21内の動作プログラムファイル23の改ざん検証は可能であるが、動作プログラムファイル23に記載されている署名情報の信頼性については閲覧者が判断することになる。閲覧者が作成者を既知であれば署名情報に記載された作成者の危険性を判断できるため、カプセル化文書ファイル21のセキュリティ機能は保たれるが、閲覧者が作成者を既知でないときには作成者の危険性を判断できないため、カプセル化文書ファイル21のセキュリティ機能が保たれない。そこで、本実施の形態においては、閲覧者が作成者を既知でないときにもカプセル化文書フ

ファイル21のセキュリティ機能を保つため、作成者側と閲覧者側が信頼できる第三者認証局を設けることによって、カプセル化文書ファイル21のセキュリティ機能を確保するようにしたのである。

【0153】

[1. コンピュータ1が備える特長的な機能の説明]

コンピュータ1が備える特長的な機能について説明する。

【0154】

[1-1. カプセル化文書作成処理]

コンピュータ1は、内蔵するCPU2がOS上で動作するアプリケーションプログラムに従うことにより、カプセル化文書ファイル21を作成するカプセル化文書作成処理を実行するカプセル化文書作成装置として機能することになる。図13は、CPU2がOS上で動作するアプリケーションプログラムに従うことにより実現されるカプセル化文書作成処理の流れを示すフローチャートである。

【0155】

図13に示すように、まず、作成者の秘密鍵・公開鍵を生成した後（ステップS51）、作成者の身元情報を作成者の公開鍵情報に記載し、作成者の公開鍵情報を第三者認証局へ送信する（ステップS52）。

【0156】

ここで、第三者認証局は、公開鍵の正当性を確認し、公開鍵証明書を発行する中立的な機関である。第三者認証局は、作成者の公開鍵情報を取得し、作成者の身元情報を保障するため、作成者の公開鍵情報へ署名情報を記載する。公開鍵の署名方法としては、取得した作成者の公開鍵情報から特徴量を算出し、特徴量を第三者認証局の秘密鍵で暗号化する方法が挙げられる。署名方法は、作成者の信頼性が証明できれば、その他の署名方法を使用しても良い。

【0157】

また、第三者認証局は、第三者認証局の秘密鍵情報によって署名した作成者の公開鍵情報を作成者に返信し、第三者認証局の公開鍵情報を閲覧者に安全な通信経路で配布する。ここで安全な経路とは、第三者認証局から閲覧者へ公開鍵を配布する途中で改ざんされないことが保障された経路を示す。第三者認証局の公開

鍵情報の配布形態としては、第三者認証局のホームページ上に掲載して自由にダウンロードできても良いし、CD-ROMやDVD-ROMなどの記憶媒体に公開鍵情報を記録して閲覧者へ配布しても良い。また、第三認証局の公開鍵情報は、閲覧者側のコンピュータに予め保持されている場合が多いので、公開鍵情報を配布せずに閲覧者側のコンピュータに保持されている公開鍵情報を使用しても良い。公開鍵情報のフォーマットとしては、規格化されている認証書フォーマット(X.509フォーマットなど)を使用しても良い。これにより、第三者認証局が作成者側の公開鍵情報を署名し、カプセル化文書ファイル21の信頼性を保証する。

【0158】

次に、第三者認証局によって署名された作成者の公開鍵情報を取得する(ステップS53)。

【0159】

以降のステップS54～S59については、第一の実施の形態で説明した図4に示すステップS1～S3、ステップS5～S7と何ら変わるものではないため、その説明は省略する。

【0160】

以上のようにして作成されたカプセル化文書ファイル21は、第三者認証局によって署名された作成者の公開鍵とともに、ネットワーク7を介して所定のコンピュータ1に対して送信されて配布されることになる。

【0161】

[1-2. 改ざん検証処理]

コンピュータ1は、内蔵するCPU2がOS内にあるShellプログラムが関連付けされている起動プログラムに従うことにより、動作プログラムファイル23の改ざん検証処理を実行する改ざん検証装置として機能することになる。ここでは、図3に示すようなカプセル化文書ファイル21が第三者認証局によって署名された作成者の公開鍵とともに別のコンピュータ1(カプセル化文書作成装置)から配布されたものとして説明する。また、第三者認証局の公開鍵情報が、閲覧者に安全な通信経路で配布されているものとする。

【0162】

閲覧者がキーボード10やマウス11等の入力装置を介してカプセル化文書ファイル21を選択した際に、OS内にあるShellプログラムが拡張子等でカプセル化文書ファイル21と判断した場合には、起動プログラムが起動する。起動プログラムは、選択されたカプセル化文書ファイル21を読み込み、カプセル化文書ファイル21内にある動作プログラムファイル23の改ざん検証をする。

【0163】

図14は、起動プログラムによる改ざん検証処理の流れを示すフローチャートである。図14に示すように、まず、配布されたカプセル化文書ファイル21と第三者認証局によって署名された作成者の公開鍵を取得して解凍すると（ステップS61）、第三者認証局の公開鍵を使用して、暗号化された作成者の公開鍵情報を復号化し（ステップS62）、作成者の公開鍵に記載されている署名情報を検証する（ステップS63）。

【0164】

第三者認証局によって保証されている場合、つまり改ざんされていない場合には（ステップS64のN）、復号化された作成者の公開鍵を使用してカプセル化文書ファイル21内にある暗号化された動作プログラムファイル23の特徴量を復号化し（ステップS65）、動作プログラムファイル23の特徴量を算出する（ステップS66）。

【0165】

次いで、ステップS67に進み、配布されたカプセル化文書ファイル21内の暗号化された動作プログラムファイル23の特徴量を復号化した値と閲覧者側で動作プログラムファイル23の特徴量を算出した値とを比較し、動作プログラムファイル23の改ざん検証を実行する。

【0166】

動作プログラムファイル23の改ざん検証を行った結果、2つの特徴量が一致していれば、すなわち動作プログラムファイル23が改ざんされていなければ（ステップS68のN）、動作プログラムファイル23に記載された署名情報をディスプレイ9に表示し（ステップS69）、表示された署名者が信用できるかを

閲覧者に判断させる。

【0167】

信用できる署名者である旨がキーボード10やマウス11等の入力装置を介して閲覧者により入力された場合には（ステップS70のY）、動作プログラムファイル23の動作プログラムを実行してディスプレイ9上にカプセル化文書ファイル21内の文書情報ファイル22を表示する（ステップS71）。

【0168】

一方、第三者認証局によって保証されていない場合（ステップS64のY）、動作プログラムファイル23が改ざんされている場合（ステップS68のY）、信用できる署名者でない旨がキーボード10やマウス11等の入力装置を介して閲覧者により入力された場合には（ステップS70のN）、動作プログラムファイル23の動作プログラムを実行せずに、不正なプログラムファイルであることを報知する不正報知処理を実行する（ステップS72）。不正報知処理としては、例えば、公開鍵が第三者認証局によって保証されていない旨やカプセル化文書ファイル21内の動作プログラムファイル23が配布途中で改ざんされたことを通知するダイアログボックスをディスプレイ9上に表示することが考えられる。

【0169】

このように本実施の形態によれば、カプセル化文書作成装置と改ざん検証装置とを備え、動作プログラムファイル23全体を暗号化処理せずとも、動作プログラムファイル23の特徴量という20バイト程度の小さなデータを暗号化処理するだけで、カプセル化文書ファイル21の配布途中における動作プログラムファイル23の改ざん検証ができる。これにより、高速にカプセル化文書ファイル21内の動作プログラムファイル23の改ざん検証が実行できる利便性の高いカプセル化文書ファイル21を提供することができる。また、第三者認証局が作成者側の公開鍵情報を署名し、カプセル化文書ファイル21の信頼性を保証することにより、閲覧者が作成者を既知でなくとも作成者の危険性を判定してカプセル化文書ファイル21のセキュリティ機能を保つことができる。

【0170】

なお、起動プログラムは、OS内にあるShellプログラムで起動するものに限

るものではなく、Shellプログラムがこの様な機能を有しても良い。

【0171】

なお、本実施の形態においては、作成者の公開鍵情報の特徴量を暗号化することによって、カプセル化文書ファイル21の安全性を保証したが、作成者の公開鍵情報を暗号化することによって、カプセル化文書ファイル21の安全性を保証するようにしても良い。

【0172】

一例として、オペレーティングシステム（OS）提供者が、作成者の公開鍵情報を暗号化する例を以下に示す。

【0173】

まず、OS提供者が、OS提供者の秘密鍵・公開鍵情報を作成し、作成者の公開鍵情報をOS提供者の秘密鍵で暗号化して、暗号化した作成者の公開鍵を作成者へ返信する。なお、OS提供者の公開鍵情報は、OSに予め保存されている。

【0174】

作成者は、作成したカプセル化文書ファイル21と暗号化された公開鍵情報を閲覧者へ送信する。

【0175】

閲覧者は、OSに予め保存されているOS提供者の公開鍵情報を使用して、暗号化された公開鍵情報を復号化し、復号化された公開鍵情報を使用して、カプセル化文書ファイル21の動作プログラムファイル23を第一の実施の形態と同様に検証することによって、安全にカプセル化文書ファイル21を使用することができる。

【0176】

作成者の公開鍵情報を暗号化する方法では、公開鍵情報が第三者の秘密鍵によって暗号化されているので、閲覧者は第三者の公開鍵情報を取得しないと、作成者の公開鍵情報を使用できないため、カプセル化文書を利用することができない。このため、作成者の公開鍵情報を暗号化する方法では、作成者は第三者を通して、閲覧者に対して課金処理などを行うことも可能となる。

【0177】

一方、作成者の公開鍵情報の特微量を暗号化する方法では、公開鍵情報は第三者の秘密鍵によって暗号化されていないので、作成者の公開鍵情報の署名情報が第三者によって証明されなくとも、閲覧者は作成者の公開鍵情報を使用するか否かの選択をして、カプセル化文書ファイル21を使用することが可能となる。

【0178】

[第四の実施の形態]

本発明の第四の実施の形態を図15または図16に基づいて説明する。なお、本発明の第一の実施の形態ないし第三の実施の形態において説明した部分と同一部分については同一符号を用い、説明も省略する。

【0179】

第一の実施の形態ないし第三の実施の形態によれば、各動作プログラムファイル23の特微量が暗号化されて保存されている特微量保持ファイル24をカプセル化文書ファイル21に保持するようにしたが、本実施の形態においては、特微量保持ファイル24をカプセル化文書ファイル21に保持せずに、OS内にあるShellプログラムが関連付けされている起動プログラムに保持するようにしたるものである。

【0180】

[1. カプセル化文書の説明]

本発明の特長の1つである文書のデータ構造（カプセル化文書構造）の概要について図15を参照して説明する。このカプセル化文書ファイル21は、コンピュータ1のHDD5に保持されている。本実施の形態のカプセル化文書ファイル21は、文書上での表現実体となる各種のコンテンツや文書構造をファイル化した文書情報ファイル22と、文書情報ファイル22を表現実体化させる動作プログラムの動作プログラムファイル23とを、单一の文書としてカプセル化手段を用いてカプセル化したものである。これらの情報は、各々一般的なコンピュータ1のOSが管理できる個別のファイル単位の構造となっている。

【0181】

より詳細には、文書情報ファイル22のコンテンツ情報は、静止画像、動画像、音声、テキストファイル等であってコンピュータ1で使用、動作出来るファイ

ルフォーマットに準じてファイル化されている。また、カプセル化手段には、Z I P、L H A等の周知のマルチファイル圧縮方式を使用し、各文書情報ファイル22を閲覧等で表示する場合はこれらのマルチファイル圧縮フォーマットで符号化されているファイルを動的に復号化することで使用する。

【0182】

動作プログラムファイル23の動作プログラムは、中間言語コードで記述されている事が望ましい。動作プログラムが中間言語で記述されていれば、この中間言語を解釈実行できるコンパイラまたはインタプリタプログラムがコンピュータにインストールされている状況においてコンピュータの機種依存性が無くなる。このような中間言語としては、java（Sun Microsystemsの登録商標）言語がある。このような動作プログラムファイル23の特徴量は、起動プログラムに保持されている。

【0183】

すなわち、第一の実施の形態ないし第三の実施の形態のカプセル化文書ファイル21と異なる点は、特徴量保持ファイル24をカプセル化文書ファイル21に保持していない点である。

【0184】

したがって、文書情報ファイル22を表現実体化させる動作プログラムファイル23が当該文書情報ファイル22と一緒にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することが可能になり、この際、配布された動作プログラムファイル23の特徴量を算出し、外部に保持されている動作プログラムファイル23の特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイル21の配布途中における動作プログラムファイル23の改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することが可能になる。

【0185】

[2. コンピュータ1が備える特長的な機能の説明]

次に、コンピュータ1が備える特長的な機能について説明する。

【0186】

[2-1. 改ざん検証処理]

コンピュータ1は、内蔵するCPU2がOS内にあるShellプログラムが関連付けされている起動プログラムに従うことにより、動作プログラムファイル23の改ざん検証処理を実行する改ざん検証装置として機能することになる。ここでは、図15に示すようなカプセル化文書ファイル21が公開鍵とともに別のコンピュータ1（カプセル化文書作成装置）から配布されたものとして説明する。

【0187】

閲覧者がキーボード10やマウス11等の入力装置を介してカプセル化文書ファイル21を選択した際に、OS内にあるShellプログラムが拡張子等でカプセル化文書ファイル21と判断した場合には、起動プログラムが起動する。起動プログラムは、選択されたカプセル化文書ファイル21を読み込み、カプセル化文書ファイル21内にある動作プログラムファイル23の改ざん検証をする。

【0188】

図16は、起動プログラムによる改ざん検証処理の流れを示すフローチャートである。図16に示すように、まず、起動プログラム内の動作プログラムファイル23の特微量を読み込む（ステップS81）。

【0189】

次に、閲覧者がキーボード10やマウス11等の入力装置を介して選択したカプセル化文書ファイル21内にある動作プログラムファイル23を読み込み（ステップS82）、動作プログラムファイル23の特微量を算出する（ステップS83）。

【0190】

次いで、ステップS84に進み、起動プログラム内の動作プログラムファイル23の特微量と閲覧者側で算出した動作プログラムファイル23の特微量とを比較し、動作プログラムファイル23の改ざん検証を実行する。

【0191】

動作プログラムファイル23の改ざん検証を行った結果、2つの特微量が一致している場合、すなわち動作プログラムファイル23が改ざんされていない場合には（ステップS85のN）、動作プログラムファイル23の動作プログラム（

文書閲覧プログラム）を起動して文書情報ファイル22をディスプレイ9に表示する（ステップS86）。

【0192】

一方、特微量検証プログラムファイルの改ざん検証を行った結果、2つの特微量が一致していない場合、すなわち特微量検証プログラムファイルが改ざんされている場合には（ステップS85のY）、特微量検証プログラムファイルが改ざんされたことを報知する不正報知処理を実行する（ステップS87）。不正報知処理としては、例えば、特微量検証プログラムファイルが改ざんされたことを通知するダイアログボックスをディスプレイ9上に表示することが考えられる。

【0193】

このように本実施の形態によれば、カプセル化文書作成装置と改ざん検証装置とを備え、動作プログラムファイル23全体を暗号化処理せずとも、カプセル化文書ファイル21の配布途中における動作プログラムファイル23の改ざん検証ができる。これにより、高速にカプセル化文書ファイル21内の動作プログラムファイル23の改ざん検証が実行できる利便性の高いカプセル化文書ファイル21を提供することができる。

【0194】

なお、起動プログラムは、OS内にあるShellプログラムで起動するものに限るものではなく、Shellプログラムがこの様な機能を有しても良い。

【0195】

また、起動プログラムがOSのShellプログラムの機能としてない場合は、閲覧者がカプセル化文書ファイル21を起動するために起動プログラムを取得することが必須となる。起動プログラムの取得方法としては、起動プログラムをインターネットからダウンロードするようにすることが考えられる。しかしながら、インターネットから起動プログラムをダウンロードする場合は、起動プログラムをダウンロードするサイトのURLを使用者が知らなければならない。そこで、このファイルのプロパティ情報としてURLを記述しておいても良いし、ファイルの先頭にURLを記述することによって、汎用のテキストエディタでも容易に起動プログラムのダウンロードサイトのURLを認識できるようにしても良

い。

【0196】

[第五の実施の形態]

本発明の第五の実施の形態を図17ないし図19に基づいて説明する。なお、本発明の第一の実施の形態ないし第三の実施の形態において説明した部分と同一部分については同一符号を用い、説明も省略する。

【0197】

[1. カプセル化文書の説明]

本発明の特長の1つである文書のデータ構造（カプセル化文書構造）の概要について図17を参照して説明する。このカプセル化文書ファイル21は、コンピュータ1のHDD5に保持されている。本実施の形態のカプセル化文書ファイル21は、文書上での表現実体となる各種のコンテンツや文書構造をファイル化した文書情報ファイル22と、文書情報ファイル22を表現実体化させる動作プログラムの動作プログラムファイル23と、特微量検証プログラムファイル25とを、単一の文書としてカプセル化手段を用いてカプセル化したものである。これらの情報は、各々一般的なコンピュータ1のOSが管理できる個別のファイル単位の構造となっている。

【0198】

より詳細には、文書情報ファイル22のコンテンツ情報は、静止画像、動画像、音声、テキストファイル等であってコンピュータ1で使用、動作出来るファイルフォーマットに準じてファイル化されている。また、カプセル化手段には、ZIP、LHA等の周知のマルチファイル圧縮方式を使用し、各文書情報ファイル22を閲覧等で表示する場合はこれらのマルチファイル圧縮フォーマットで符号化されているファイルを動的に復号化することで使用する。

【0199】

動作プログラムファイル23の動作プログラムは、中間言語コードで記述されている事が望ましい。動作プログラムが中間言語で記述されていれば、この中間言語を解釈実行できるコンパイラまたはインタプリタプログラムがコンピュータにインストールされている状況においてコンピュータの機種依存性が無くなる。

このような中間言語としては、java（Sun Microsystemsの登録商標）言語がある。
。

【0200】

特微量検証プログラムファイル25は、動作プログラムファイル23の改ざん検証を実行するものである。このような特微量検証プログラムファイルの特微量は、起動プログラムに保持されている。

【0201】

すなわち、第一の実施の形態ないし第三の実施の形態のカプセル化文書ファイル21と異なる点は、特微量検証プログラムファイル25をカプセル化文書ファイル21に保持している点である。

【0202】

[2. コンピュータ1が備える特長的な機能の説明]

次に、コンピュータ1が備える特長的な機能について説明する。本実施の形態の特長的な処理は、カプセル化文書ファイル21に保持されている特微量検証プログラムファイル25を外部の起動プログラムから起動して動作させることにより、動作プログラムファイル23の改ざん検証処理を実行するものである。

【0203】

[2-1. 改ざん検証処理]

コンピュータ1は、内蔵するCPU2がOS内にあるShellプログラムが関連付けられている起動プログラムに従うことにより、動作プログラムファイル23の改ざん検証処理を実行する改ざん検証装置として機能することになる。ここでは、図17に示すようなカプセル化文書ファイル21が公開鍵とともに別のコンピュータ1（カプセル化文書作成装置）から配布されたものとして説明する。

【0204】

閲覧者がキーボード10やマウス11等の入力装置を介してカプセル化文書ファイル21を選択した際に、OS内にあるShellプログラムが拡張子等でカプセル化文書ファイル21と判断した場合には、起動プログラムが起動する。起動プログラムは、選択されたカプセル化文書ファイル21を読み込み、カプセル化文書ファイル21内にある動作プログラムファイル23の改ざん検証をする。

【0205】

図18は、起動プログラムによる改ざん検証処理の流れを示すフローチャートである。図18に示すように、まず、起動プログラム内の特微量検証プログラムファイル25の特微量を読み込む（ステップS91）。

【0206】

次に、閲覧者がキーボード10やマウス11等の入力装置を介して選択したカプセル化文書ファイル21内にある特微量検証プログラムファイル25を読み込み（ステップS92）、特微量検証プログラムファイル25の特微量を算出する（ステップS93：特微量算出手段）。

【0207】

次いで、ステップS94に進み、起動プログラム内の特微量検証プログラムファイル25の特微量と閲覧者側で算出した特微量検証プログラムファイル25の特微量とを比較し、特微量検証プログラムファイル25の改ざん検証を実行する。

【0208】

特微量検証プログラムファイル25の改ざん検証を行った結果、2つの特微量が一致している場合、すなわち特微量検証プログラムファイル25が改ざんされていない場合には（ステップS95のN：判定手段）、特微量検証プログラムを実行する（ステップS96：改ざん検証実行手段）。

【0209】

一方、特微量検証プログラムファイル25の改ざん検証を行った結果、2つの特微量元素が一致していない場合、すなわち特微量検証プログラムファイル25が改ざんされている場合には（ステップS95のY：判定手段）、特微量検証プログラムファイル25が改ざんされたことを報知する不正報知処理を実行する（ステップS97）。不正報知処理としては、例えば、特微量検証プログラムファイル25が改ざんされたことを通知するダイアログボックスをディスプレイ9上に表示することが考えられる。

【0210】

ここで、ステップS96での特微量検証プログラムを実行することにより実現

される特微量検証処理について説明する。図19は、特微量検証処理の流れを示すフローチャートである。図19に示すように、まず、同じカプセル化文書ファイル21内の動作プログラムファイル23及び特微量保持ファイル24をすべて読み込み（ステップS101）、取得した公開鍵を使用して暗号化された特微量を復号化するとともに（ステップS102）、動作プログラムファイル23の特微量を算出する（ステップS103）。

【0211】

次いで、ステップS104に進み、復号化した動作プログラムファイル23の特微量と閲覧者側で算出した動作プログラムファイル23の特微量とを比較し、動作プログラムファイル23の改ざん検証を実行する。

【0212】

動作プログラムファイル23の改ざん検証を行った結果、2つの特微量が一致している場合、すなわち動作プログラムファイル23が改ざんされていない場合には（ステップS105のN）、動作プログラムファイル23の動作プログラム（文書閲覧プログラム）を起動して文書情報ファイル22をディスプレイ9に表示する（ステップS106）。

【0213】

一方、動作プログラムファイル23の改ざん検証を行った結果、2つの特微量が一致していない場合、すなわち動作プログラムファイル23が改ざんされている場合には（ステップS105のY）、動作プログラムファイル23が改ざんされたことを報知する不正報知処理を実行する（ステップS107）。不正報知処理としては、例えば、動作プログラムファイル23が改ざんされたことを通知するダイアログボックスをディスプレイ9上に表示することが考えられる。

【0214】

このように本実施の形態によれば、カプセル化文書ファイル21内に特微量検証プログラムファイル25を挿入し、起動プログラムが特微量検証プログラムファイル25の改ざん検証と特微量検証プログラム25の起動とを実行することにより、カプセル化文書ファイル21内にある複数の動作プログラムファイル23の全てに対して改ざん検証を行うことが可能となる。

【0215】

なお、起動プログラムは、OS内にあるShellプログラムで起動するものに限るものではなく、Shellプログラムがこの様な機能を有しても良い。

【0216】

また、起動プログラムがOSのShellプログラムの機能としてない場合は、閲覧者がカプセル化文書ファイル21を起動するために起動プログラムを取得することが必須となる。起動プログラムの取得方法としては、起動プログラムをインターネットからダウンロードするようにすることが考えられる。しかしながら、インターネットから起動プログラムをダウンロードする場合は、起動プログラムをダウンロードするサイトのURLを使用者が知らなければならない。そこで、このファイルのプロパティ情報としてURLを記述しておいても良いし、ファイルの先頭にURLを記述することによって、汎用のテキストエディタでも容易に起動プログラムのダウンロードサイトのURLを認識できるようにしても良い。

【0217】

なお、各実施の形態においては、暗号化と復号化の鍵情報が異なる公開鍵暗号方式により動作プログラムファイル23の特徴量等を暗号化するようにしたが、これに限るものではなく、暗号化と復号化の鍵情報が同一である秘密鍵暗号方式により動作プログラムファイル23の特徴量等を暗号化するようにしても良い。すなわち、カプセル化文書ファイル21を閲覧する閲覧者のコンピュータ1には、動作プログラムファイル23の特徴量等を暗号化した鍵情報が保持されることになる。したがって、各閲覧者のコンピュータ1には、異なる鍵情報が必要となる。なお、この鍵情報は秘密にすることが前提なので、カプセル化文書ファイル21内に鍵情報を添付して配布することはできない。これにより、暗号化鍵と復号化鍵とが同一の鍵であることにより、暗号化や復号化を高速に実行することが可能になる。

【0218】**【発明の効果】**

請求項1記載の発明のプログラム改ざん検証方法によれば、動作プログラムファイル全体を暗号化処理せずとも、動作プログラムファイルの特徴量という小さ

なデータ（20バイト程度）を暗号化処理するだけで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が行えるので、動作プログラムファイルの改ざん検証を高速に行うことができる。

【0219】

請求項2記載の発明のプログラム改ざん検証方法によれば、動作プログラムファイル全体を暗号化処理せずとも、動作プログラムファイルの特徴量という小さなデータ（20バイト程度）を暗号化処理するだけで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が行えるので、動作プログラムファイルの改ざん検証を高速に行うことができる。

【0220】

請求項3記載の発明のカプセル化文書構造によれば、各種ファイルで構成されるファイル群とファイル群を構成する所定のファイルに関する暗号化された特徴量を保持する特徴量保持ファイルとが一元的に管理されていることにより、カプセル化文書ファイルを配布する際に、所定のファイルの暗号化特徴量を復号化するとともに配布された所定のファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中におけるファイルの改ざん検証を行うことができる。

【0221】

請求項4記載の発明のカプセル化文書構造によれば、文書情報ファイルを表現実体化させる動作プログラムファイルが当該文書情報ファイルと一緒にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することができ、この際、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに配布された動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証ができるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することができる。

【0222】

請求項5記載の発明のカプセル化文書構造によれば、文書情報ファイルを表現

実体化させる動作プログラムファイルの保存位置を示す位置情報が当該文書情報ファイルと一緒にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することができ、この際、特微量保持ファイルに保持されている動作プログラムファイルの暗号化特微量を復号化するとともに所定位置に保存されている動作プログラムファイルの特微量を算出し、復号化した特微量と算出されたファイルの特微量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することができる。

【0223】

請求項6記載の発明のカプセル化文書構造によれば、文書情報ファイルを表現実体化させる動作プログラムファイルが当該文書情報ファイルと一緒にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することができ、この際、配布された動作プログラムファイルの特微量を算出し、外部に保持されている動作プログラムファイルの特微量と算出されたファイルの特微量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証が可能になるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することができる。

【0224】

請求項7記載の発明のカプセル化文書構造によれば、文書情報ファイルを表現実体化させる動作プログラムファイルの保存位置を示す位置情報が当該文書情報のファイルと一緒にカプセル化されているので、作成者のコンピュータと異なる環境でも当該文書を閲覧することができ、この際、所定位置に保存されている動作プログラムファイルの特微量を算出し、外部に保持されている動作プログラムファイルの特微量と算出されたファイルの特微量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証ができるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することができる。

【0225】

請求項8記載の発明によれば、請求項3ないし5の何れか一記載のカプセル化

文書構造において、前記特微量保持ファイルには、前記文書情報ファイルに関する暗号化された特微量も保持されていることにより、動作プログラムファイルの改ざん検証のみならず、文書情報ファイルの改ざん検証が可能になるので、更に安全に文書を閲覧することができる。

【0226】

請求項9記載の発明によれば、請求項3ないし5の何れか一記載のカプセル化文書構造において、前記特微量保持ファイルには、前記動作プログラムファイルに関する暗号化された特微量に対応付けられて前記暗号化された特微量を復号化する復号化鍵情報が保持されていることにより、閲覧者はカプセル化文書ファイルを取得するだけで動作プログラムファイル等の改ざん検証を行うことができる。

【0227】

請求項10記載の発明によれば、請求項3ないし5の何れか一記載のカプセル化文書構造において、前記特微量保持ファイルには、前記動作プログラムファイルに関する暗号化された特微量に対応付けられて前記暗号化された特微量を復号化する復号化鍵情報の保存位置を示す位置情報が保持されていることにより、閲覧者はカプセル化文書ファイルを取得するだけで動作プログラムファイル等の改ざん検証を行うことができる。

【0228】

請求項11記載の発明によれば、請求項9または10記載のカプセル化文書構造において、各動作プログラムファイル毎に異なる前記復号化鍵情報が対応付けられていることにより、例えば1つのベンダーだけでなく複数のベンダーによって複数の動作プログラムファイルが作成されるような場合、閲覧者は、各ベンダーの復号化鍵情報を使用することによって動作プログラムファイルの改ざん検証を行うことができるので、ベンダーごとに作成した動作プログラムファイルに対して、責任を持たせることが可能なカプセル化文書ファイルを提供することができる。

【0229】

請求項12記載の発明によれば、請求項3ないし11の何れか一記載のカプセ

ル化文書構造において、前記動作プログラムファイルに関する特徴量は、公開鍵暗号方式により暗号化されていることにより、カプセル化文書ファイルの生成者が所有して公開しない秘密鍵を暗号化鍵とし、秘密鍵とは異なる公開鍵を復号化鍵として閲覧者に公開することで、公開鍵を有する者だけが動作プログラムファイルに関する特徴量を復号化することができる。

【0230】

請求項13記載の発明によれば、請求項12記載のカプセル化文書構造において、前記復号化鍵情報は、第三者認証局により署名暗号化されていることにより、第三者認証局が作成者側の復号化鍵情報（公開鍵情報）を署名し、カプセル化文書ファイルの信頼性を保証することで、閲覧者が作成者を既知でなくとも作成者の危険性を判定してカプセル化文書ファイルのセキュリティ機能を保つことができる。

【0231】

請求項14記載の発明によれば、請求項3ないし11の何れか一記載のカプセル化文書構造において、前記動作プログラムファイルに関する特徴量は、秘密鍵暗号方式により暗号化されていることにより、暗号化鍵と復号化鍵とが同一の鍵であるので、暗号化や復号化を高速に実行することができる。

【0232】

請求項15記載の発明によれば、請求項3ないし14の何れか一記載のカプセル化文書構造において、カプセル化文書ファイル内に特徴量検証プログラムファイルを挿入し、起動プログラムが特徴量検証プログラムファイルの改ざん検証と特徴量検証プログラムの起動とを実行することにより、カプセル化文書ファイル内にある複数の動作プログラムファイルの全てに対して改ざん検証を行うことができる。

【0233】

請求項16記載の発明の記憶媒体によれば、請求項3ないし15の何れか一記載のカプセル化文書構造のカプセル化文書ファイルを格納したことにより、請求項3ないし15の何れか一記載の発明と同様の作用効果を奏する。

【0234】

請求項 17 記載の発明のカプセル化文書作成装置によれば、セキュリティ性の高い請求項 4 記載のファイル構造のカプセル化文書ファイルを簡単に作成することができる。

【0235】

請求項 18 記載の発明によれば、請求項 17 記載のカプセル化文書作成装置において、セキュリティ性の高い請求項 8 記載のファイル構造のカプセル化文書ファイルを簡単に作成することができる。

【0236】

請求項 19 記載の発明の改ざん検証装置によれば、請求項 3 ないし 15 の何れか一記載のカプセル化文書構造のカプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、動作プログラムファイルの改ざん検証を実行することにより、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証ができるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することができる。

【0237】

請求項 20 記載の発明によれば、請求項 19 記載の改ざん検証装置において、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに配布された動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証を行うことができる。

【0238】

請求項 21 記載の発明によれば、請求項 19 記載の改ざん検証装置において、配布された動作プログラムファイルの特徴量を算出し、起動プログラム内の特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証を行うことができる。

【0239】

請求項 22 記載の発明によれば、請求項 19 記載の改ざん検証装置において、配布された動作プログラムファイルの特徴量を算出するとともに算出された動作

プログラムファイルの特微量を暗号化し、この暗号化した特微量と特微量保持ファイルに保持されている動作プログラムファイルの暗号化特微量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証を行うことができる。

【0240】

請求項23記載の発明によれば、請求項19記載の改ざん検証装置において、配布されたカプセル化文書ファイルに保持された特微量検証プログラムファイルの特微量を算出し、起動プログラム内の特微量検証プログラムファイル特微量と算出されたファイルの特微量とを比較することで、カプセル化文書ファイルの配布途中における特微量検証プログラムファイルの改ざん検証が可能になり、改ざんがなされていない場合に特微量検証プログラムの起動を実行することにより、カプセル化文書ファイル内にある複数の動作プログラムファイルの全てに対して改ざん検証を行うことができる。

【0241】

請求項24記載の発明のカプセル化文書作成処理プログラムによれば、セキュリティ性の高い請求項4記載のファイル構造のカプセル化文書ファイルを簡単に作成することができる。

【0242】

請求項25記載の発明によれば、請求項24記載のカプセル化文書作成処理プログラムにおいて、セキュリティ性の高い請求項8記載のファイル構造のカプセル化文書ファイルを簡単に作成することができる。

【0243】

請求項26記載の発明の記憶媒体によれば、請求項24または25記載のカプセル化文書作成処理プログラムを記憶することにより、この記憶媒体に記憶されたカプセル化文書作成処理プログラムをコンピュータに読み取らせてことで、セキュリティ性の高い請求項4または8記載のファイル構造のカプセル化文書ファイルを簡単に作成することができる。

【0244】

請求項27記載の発明の起動プログラムによれば、請求項3ないし15の何れ

か一記載のカプセル化文書構造のカプセル化文書ファイルに保持された文書情報ファイルを表現実体化させる動作プログラムファイルの特徴量に基づき、動作プログラムファイルの改ざん検証を実行することにより、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証ができるので、悪意のあるプログラムの混入を防止して安全に文書を閲覧することができる。

【0245】

請求項28記載の発明によれば、請求項27記載の起動プログラムにおいて、特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量を復号化するとともに配布された動作プログラムファイルの特徴量を算出し、復号化した特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証を行うことができる。

【0246】

請求項29記載の発明によれば、請求項27記載の起動プログラムにおいて、配布された動作プログラムファイルの特徴量を算出し、起動プログラム内の特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証を行うことができる。

【0247】

請求項30記載の発明によれば、請求項27記載の起動プログラムにおいて、配布された動作プログラムファイルの特徴量を算出するとともに算出された動作プログラムファイルの特徴量を暗号化し、この暗号化した特徴量と特徴量保持ファイルに保持されている動作プログラムファイルの暗号化特徴量とを比較することで、カプセル化文書ファイルの配布途中における動作プログラムファイルの改ざん検証を行うことができる。

【0248】

請求項31記載の発明によれば、請求項27記載の起動プログラムにおいて、配布されたカプセル化文書ファイルに保持された特徴量検証プログラムファイルの特徴量を算出し、起動プログラム内の特徴量検証プログラムファイル特徴量と算出されたファイルの特徴量とを比較することで、カプセル化文書ファイルの配

本途中における特微量検証プログラムファイルの改ざん検証を行うことができ、改ざんがなされていない場合に特微量検証プログラムの起動を実行することにより、カプセル化文書ファイル内にある複数の動作プログラムファイルの全てに対して改ざん検証を行うことができる。

【0249】

請求項32記載の発明の記憶媒体によれば、請求項27ないし31のいずれか一記載の起動プログラムを記憶することにより、この記憶媒体に記憶されたカプセル化文書作成処理プログラムをコンピュータに読み取らせることで、請求項27ないし31のいずれか一記載の発明と同様の作用効果を奏する。

【図面の簡単な説明】

【図1】

本発明の第一の実施の形態も適用される一般的又は標準的なパーソナルコンピュータを示すハードウェア構成図である。

【図2】

OSの役割の概要を示す模式図である。

【図3】

カプセル化文書ファイルのデータ構造を示す模式図である。

【図4】

カプセル化文書作成処理の流れを示すフローチャートである。

【図5】

特微量保持ファイルの例を示す説明図である。

【図6】

改ざん検証処理の流れを示すフローチャートである。

【図7】

動作権限の種類と動作権限モードとの対応関係を示す説明図である。

【図8】

特微量保持ファイルの例を示す説明図である。

【図9】

特微量保持ファイルの例を示す説明図である。

【図10】

本発明の第二の実施の形態のカプセル化文書ファイルのデータ構造を示す模式図である。

【図11】

カプセル化文書作成処理の流れを示すフローチャートである。

【図12】

改ざん検証処理の流れを示すフローチャートである。

【図13】

本発明の第三の実施の形態のカプセル化文書作成処理の流れを示すフローチャートである。

【図14】

改ざん検証処理の流れを示すフローチャートである。

【図15】

本発明の第四の実施の形態のカプセル化文書ファイルのデータ構造を示す模式図である。

【図16】

改ざん検証処理の流れを示すフローチャートである。

【図17】

本発明の第五の実施の形態のカプセル化文書ファイルのデータ構造を示す模式図である。

【図18】

改ざん検証処理の流れを示すフローチャートである。

【図19】

特微量検証処理の流れを示すフローチャートである。

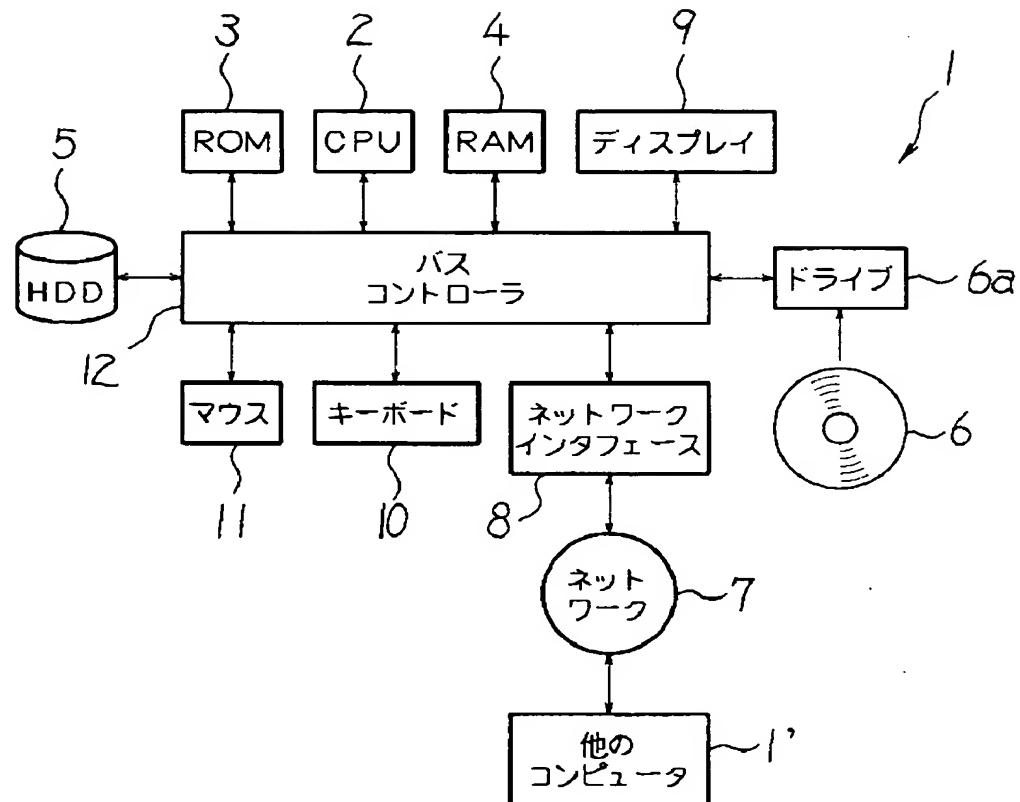
【符号の説明】

- 1 カプセル化文書作成装置、改ざん検証装置
- 2 情報処理部
- 6 記憶媒体
- 21 カプセル化文書ファイル

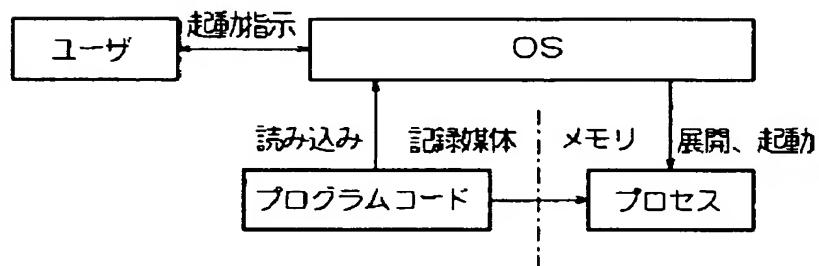
- 2 2 文書情報ファイル
- 2 3 動作プログラムファイル
- 2 4 特微量保持ファイル
- 2 5 特微量検証プログラムファイル

【書類名】 図面

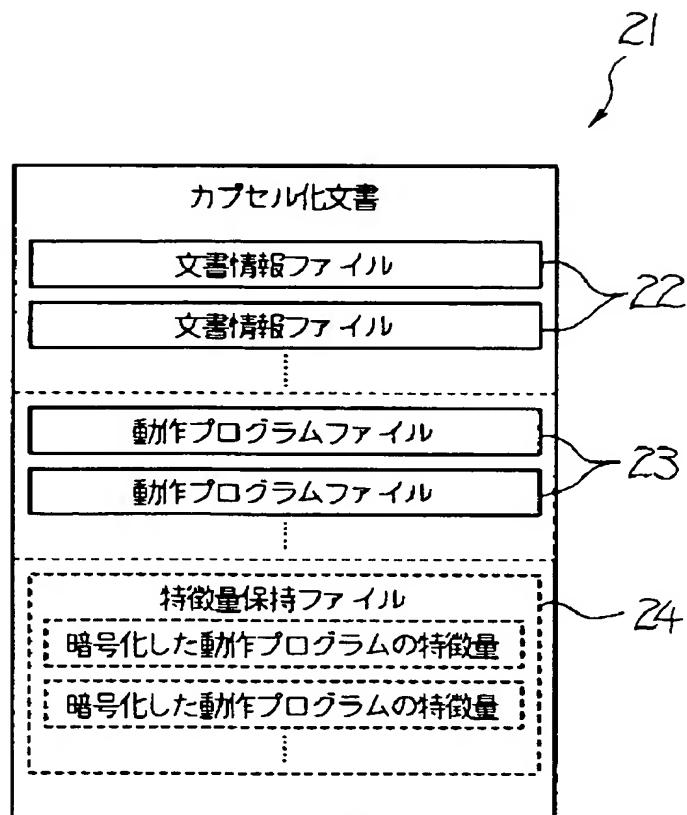
【図 1】



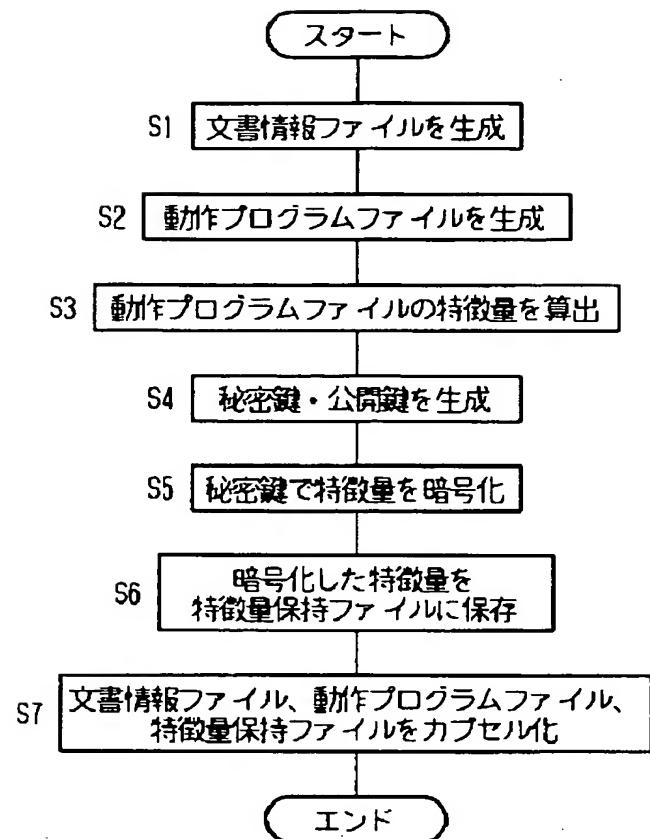
【図 2】



【図3】



【図 4】



【図5】

24
↓

<特微量ファイル>

<特微量算出情報 アルゴリズム="SHA-1"/>

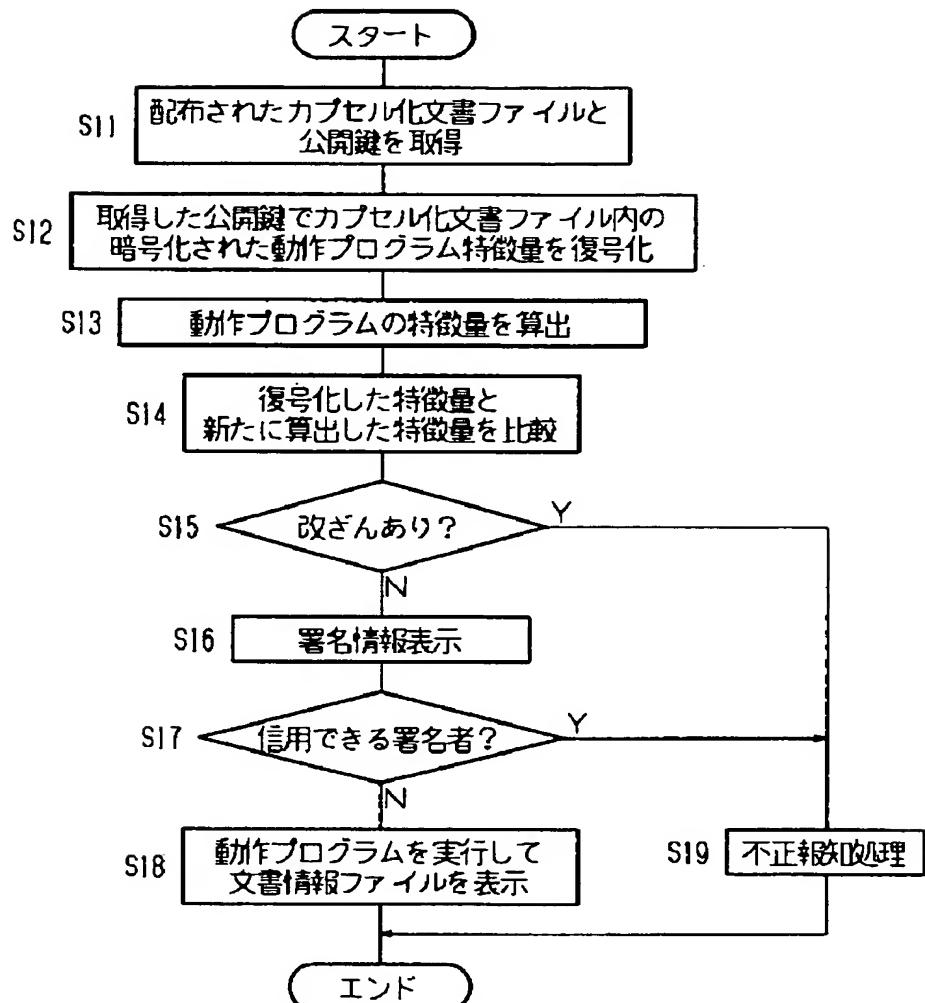
<動作プログラム1 動作プログラム名="文書作成プログラム"
特微量="8KBDi/AdAonBKtutzspftk4t/qc="<動作プログラム2 動作プログラム名="文書閲覧プログラム"
特微量="8KBDi/setasetutwetsptaett/qc="<動作プログラム3 動作プログラム名="動作検証プログラム"
特微量="8KBDi/tajeiue4tuztspfetset/qc="

⋮

<動作プログラム10 動作プログラム名="音楽再生プログラム"
特微量="8KBDi/AderetstKtutzsfetsfy/qc="

</特微量ファイル>

【図 6】



【図 7】

動作権限の種類	動作権限モード				
	A	B	C	D	
カプセル化文書内のファイルの読み込み	×	○	○	○	
コンピュータ内のファイルの読み込み	×	×	○	○	
カプセル化文書内のファイルの読み書き	×	×	×	○	-----
コンピュータ内のファイルの読み書き	×	×	×	×	
ネットワークのパケットの受信	×	×	×	×	
ネットワークのパケットの送信	×	×	×	×	
⋮					

【図8】

24
↓

<特微量ファイル>

<特微量算出情報 アルゴリズム="SHA-1"/>

<動作プログラム1 動作プログラム名="文書作成プログラム"
特微量="8KBDi/AdAonBKtuztsptk4t/qc="
公開鍵情報="adklisad49SSDgms"/><動作プログラム2 動作プログラム名="文書閲覧プログラム"
特微量="8KBDi/setasetutwetsptaett/qc="
公開鍵情報="SBSdatajsDgms4g"/><動作プログラム3 動作プログラム名="動作検証プログラム"
特微量="8KBDi/tajeiue4tuztspfetset/qc="
公開鍵情報="www.xxxxx.co.jp/location3/Key"/>

⋮

<動作プログラム10 動作プログラム名="音楽再生プログラム"
特微量="8KBDi/AderetstKtuztsfetsfy/qc="
公開鍵情報="rttszrgrgklsadees3"/>

</特微量ファイル>

【図 9】

24
↓

<特微量ファイル>

<特微量算出情報 アルゴリズム="SHA-1"/>

<動作プログラム1 動作プログラム名="文書作成プログラム"

位置情報="www.xxxxx.co.jp/location1/"

特微量="8KBDi/AdAon8KtuztspfIk4t/qc="

公開鍵情報="adkl sad49SSDgms"/>

<動作プログラム2 動作プログラム名="文書閲覧プログラム"

位置情報="www.xxxxx.co.jp/location2/"

特微量="8KBDi/setasetutwetsptaett/qc="

公開鍵情報="S8SdatajsDgms4g"/>

<動作プログラム3 動作プログラム名="動作検証プログラム"

位置情報="www.xxxxx.co.jp/location3/"

特微量="8KBDi/tajeiue4tuztspfetset/qc="

公開鍵情報="www.xxxxx.co.jp/location3/Key"/>

|

<動作プログラム10 動作プログラム名="音楽再生プログラム"

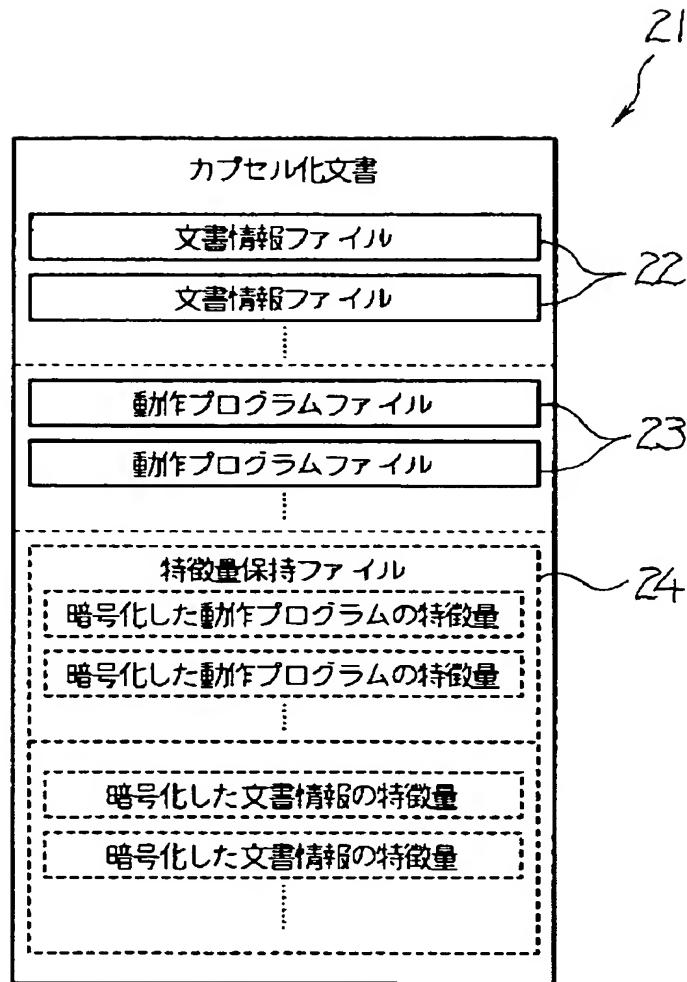
位置情報="www.xxxxx.co.jp/location10/"

特微量="8KBDi/AderetstKtuztsfetsfy/qc="

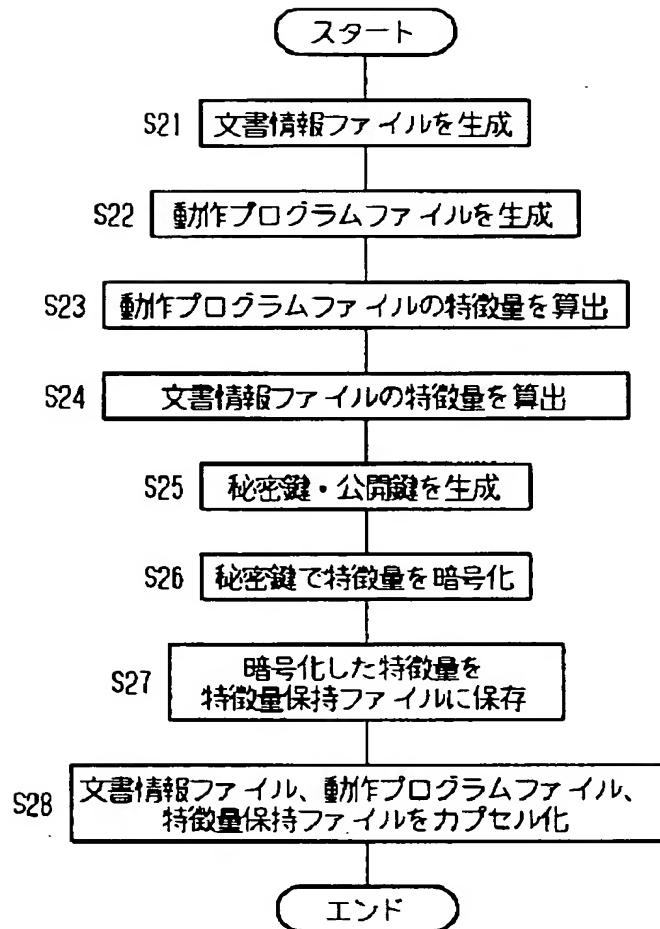
公開鍵情報="rttszrgrgklsadees3"/>

</特微量ファイル>

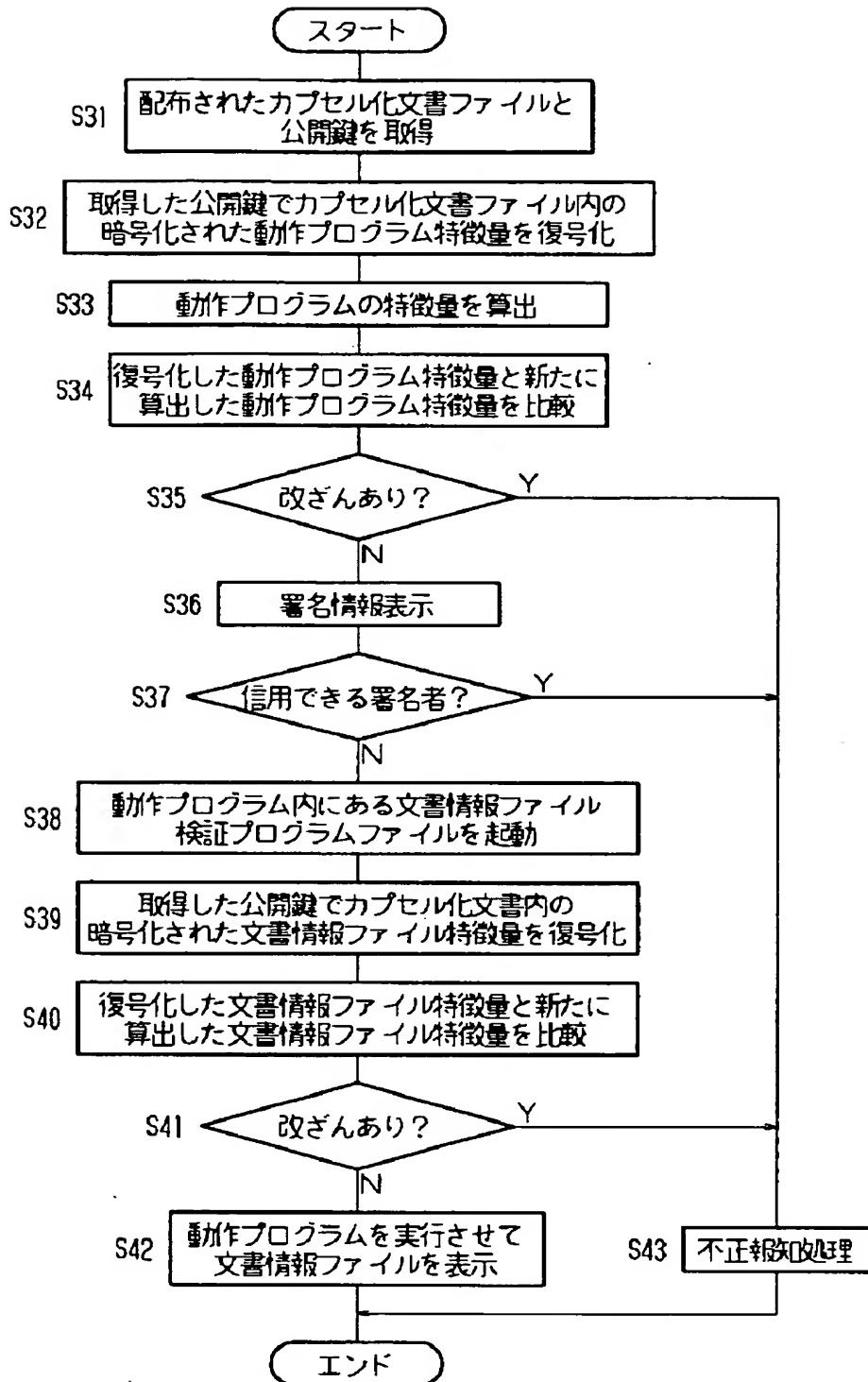
【図 10】



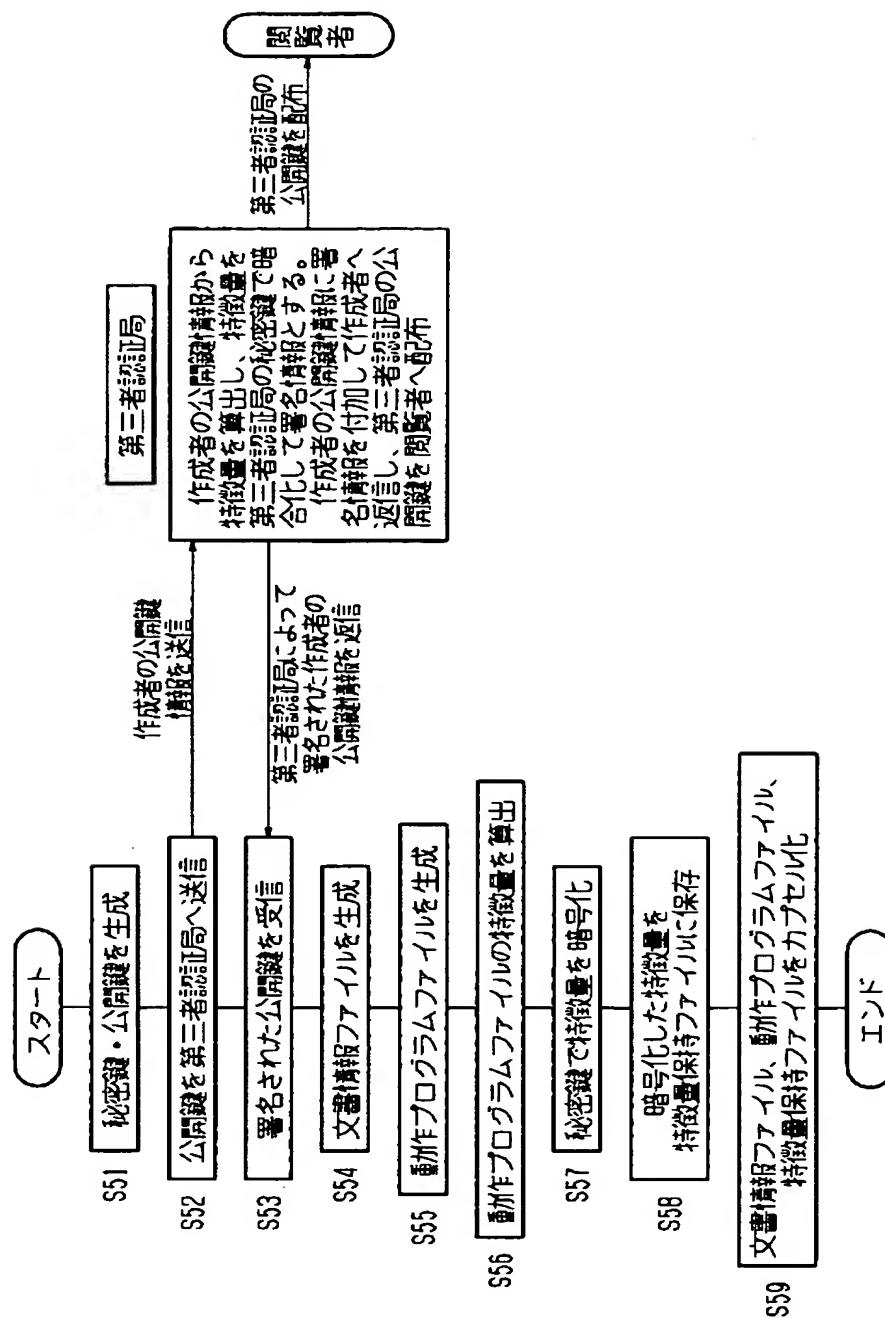
【図 1-1】



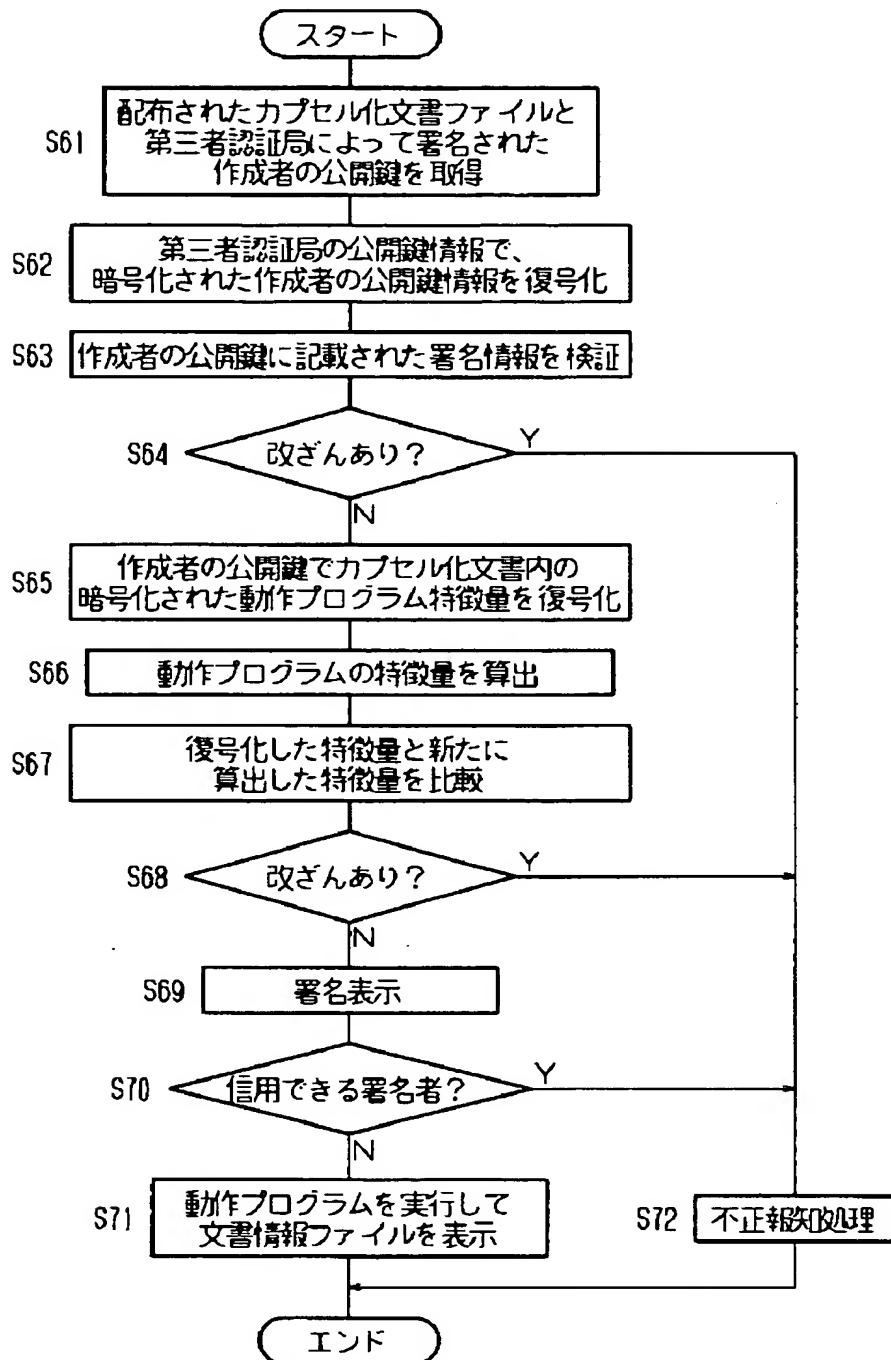
【図12】



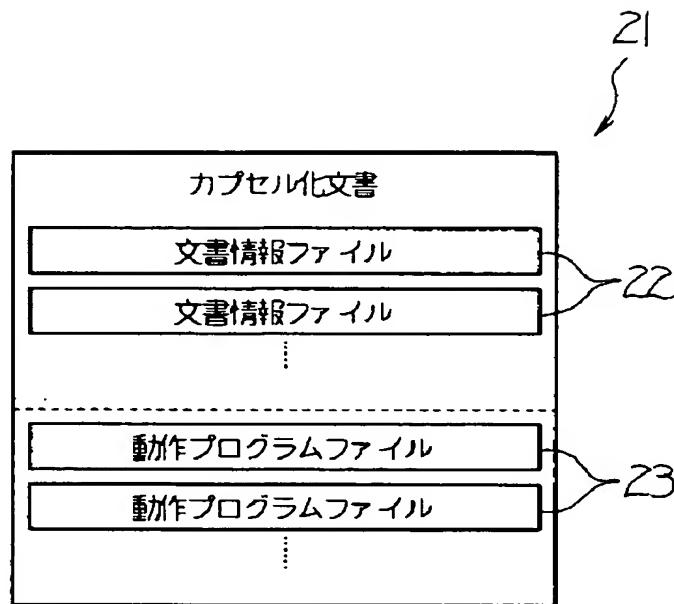
【図 13】



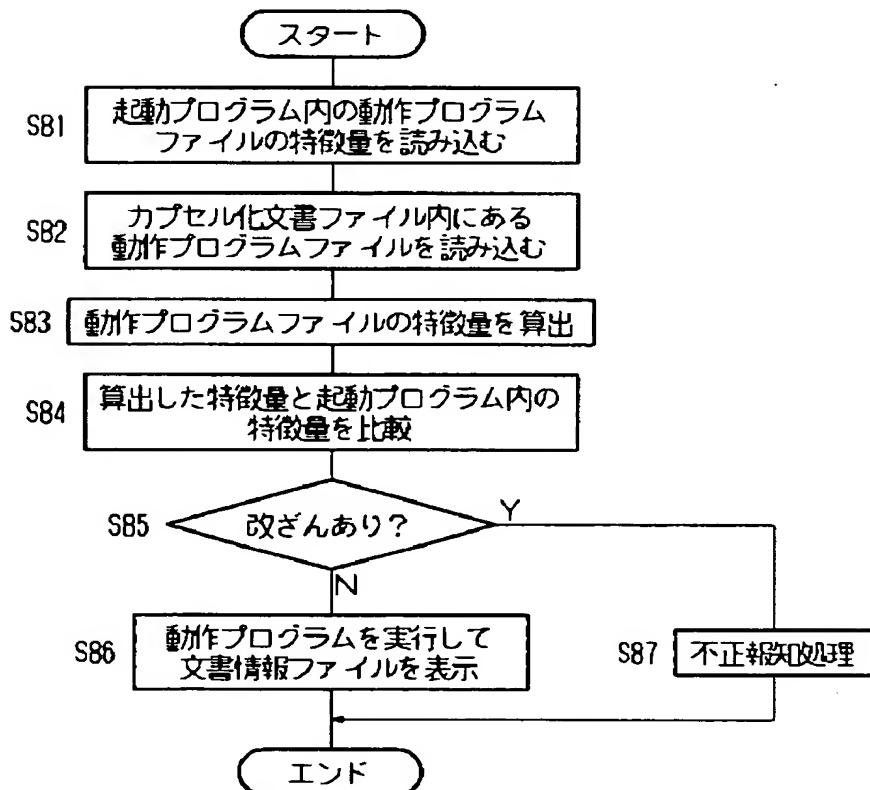
【図14】



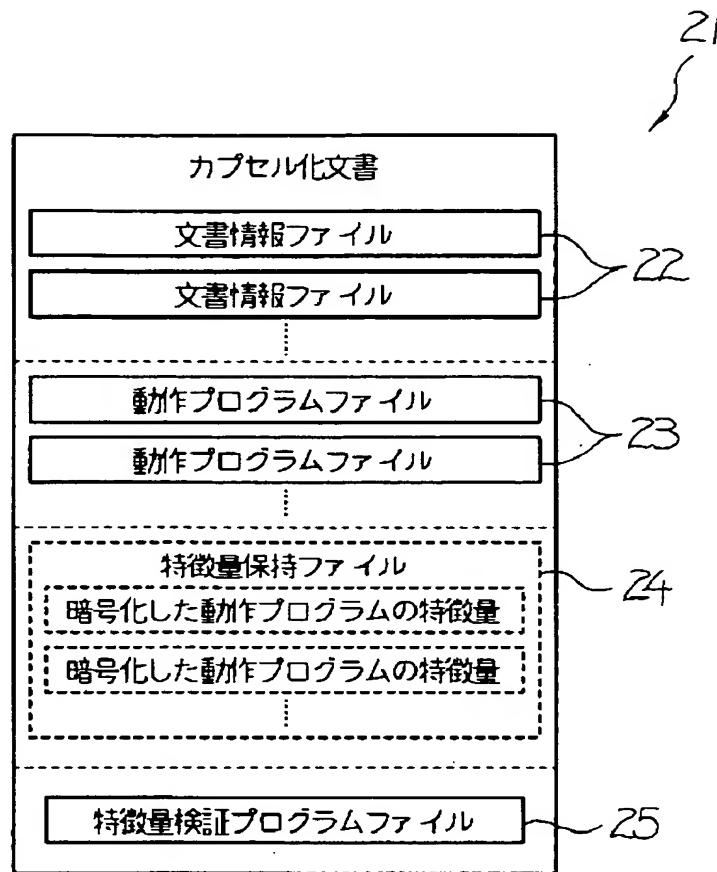
【図 15】



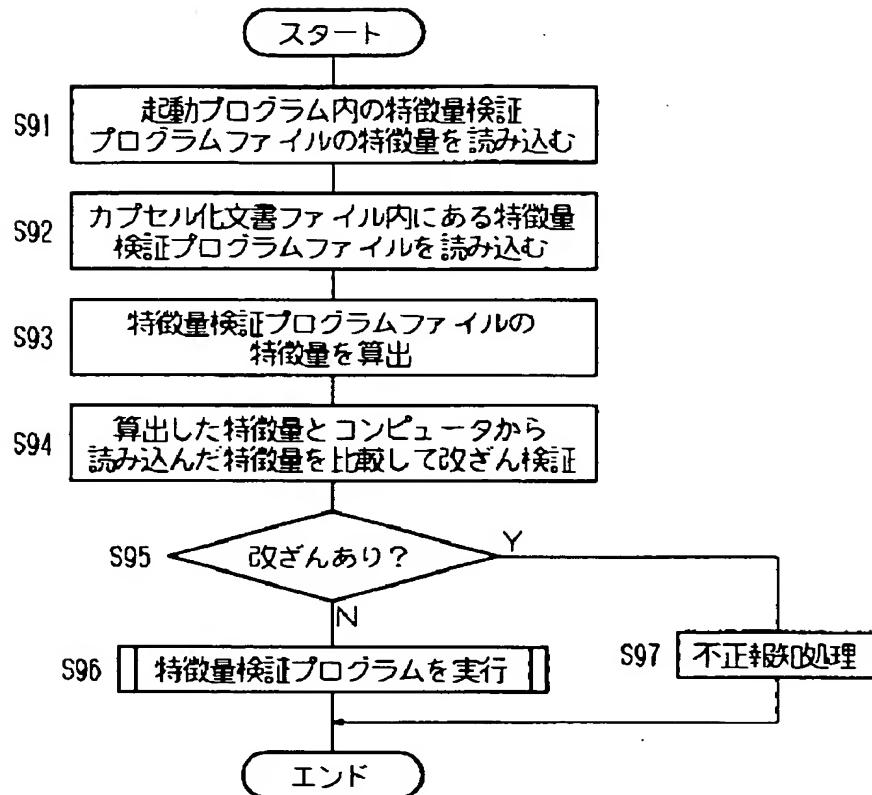
【図 16】



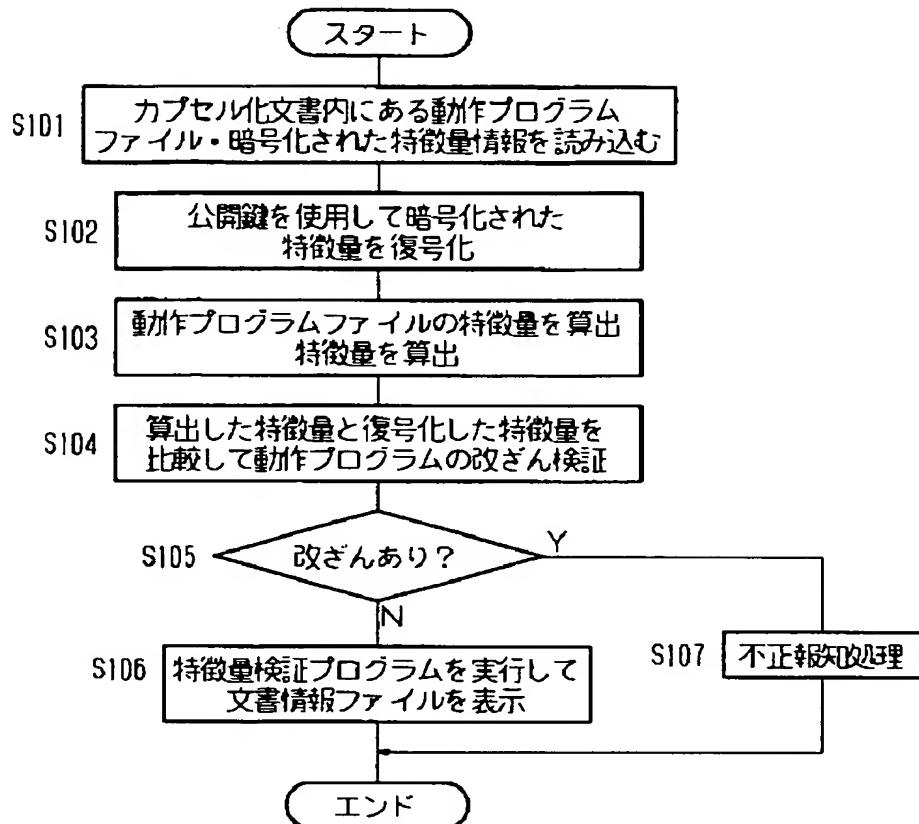
【図 17】



【図18】



【図19】



【書類名】 要約書

【要約】

【課題】 コンピュータの動作環境に左右されず、かつ、悪意のあるプログラムの混入を防止できる文書構造を提供する。

【解決手段】 文書上での表現実体となるコンテンツ情報である文書情報ファイル22と、この文書情報ファイルを表現実体化させる動作プログラムである動作プログラムファイル23と、この動作プログラムファイル23に関する暗号化された特微量を保持する特微量保持ファイル24と、をカプセル化手段によってカプセル化する。これにより、作成者のコンピュータと異なる環境でも当該文書を閲覧することができ、この際、特微量保持ファイル24に保持されている動作プログラムファイル23の暗号化特微量を復号化するとともに配布された動作プログラムファイル23の特微量を算出し、復号化した特微量と算出されたファイルの特微量とを比較することで、カプセル化文書ファイル21の配布途中における動作プログラムファイルの改ざん検証ができる。

【選択図】 図3

特願2003-195626

出願人履歴情報

識別番号 [000006747]

1. 変更年月日 2002年 5月17日

[変更理由] 住所変更

住 所 東京都大田区中馬込1丁目3番6号
氏 名 株式会社リコー